PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

Nota introdutória

O Decreto-Lei n.º 109-E/2021, de 9 de dezembro, estabeleceu a obrigatoriedade de que as empresas com sede em território nacional, que empreguem mais de 50 colaboradores elaborassem Planos de Prevenção de Riscos de corrupção e Infrações Conexas, ou PPR.

Em cumprimento com o disposto na lei, o **Grupo CAC** elaborou o presente PPR, que pretende identificar, analisar e classificar os riscos de e situações que possam expor o **Grupo CAC** a atos de corrupção e infrações conexas e as medidas preventivas e corretivas que permitam mitigar os riscos identificados.

O presente Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, em paralelo com as ações de divulgação das normas, políticas e procedimentos internos e do Código de Conduta, passarão a constituir, no **Grupo CAC**, o referencial normativo e de valores pelo qual se pautará a ação quotidiana dos dirigentes e colaboradores, dando-lhes a conhecer os procedimentos em vigor e as suas responsabilidades.

Acompanhamento, Avaliação e Monitorização do PPR

É da responsabilidade do Responsável pelo Cumprimento Normativo a monitorização e controlo da aplicação do Programa de Cumprimento Normativo, a sua revisão, controlo e execução do PPR.

O cargo de Responsável pelo Cumprimento é exercido por Natália Martins, com acesso à informação interna e meios humanos e técnicos necessários ao bom desempenho das suas funções.

Nos termos previstos nas alíneas a) e b) do n.º 4 do artigo 6º do Decreto-lei n.º 109-E/2021, de 9 de dezembro, a execução do PPR está sujeita aos seguintes controlos:

a) Elaboração de relatório de avaliação intercalar nas situações identificadas de risco elevado ou máximo;

b) Elaboração de relatório de avaliação anual, contendo nomeadamente a quantificação do grau de implementação das medidas preventivas e corretivas identificadas, bem como a previsão da sua plena implementação.

O acompanhamento anual do Plano deve basear-se na análise das denúncias recebidas através do canal implementado para o efeito, através de ações específicas de avaliação dos riscos identificados e através da análise de indicadores, especialmente preparados para o efeito.

O processo de acompanhamento deve garantir que são implementados os mecanismos de controlo adequados para as atividades da organização e que os procedimentos sejam compreendidos e seguidos em todos os níveis.

Abordagem e âmbito

O processo de identificação de riscos e infrações conexas, teve como base, a identificação das áreas e processos relevantes da organização em matéria de corrupção e infrações conexas, à análise das relações com entidades terceiras, públicas ou privadas, tendo como principal objetivo a identificação, análise e classificação dos riscos e das situações que possam expor o **Grupo CAC** a atos de corrupção e infrações conexas.

Este trabalho foi realizado com base em documentação e entrevistas com diversos responsáveis das direções e Administração. As áreas de risco identificadas estão melhor descritas no quadro anexo.

Metodologia

A metodologia de cálculo dos riscos utilizada na Análise de Risco do **Grupo CAC** baseia-se nas boas práticas do Quadro Nacional de Referência para a Cibersegurança (QNRCS), e os principais referenciais em matéria de gestão de riscos como a ISO\IEC 27005 e a NP ISO/IEC 31000.

O Quadro Nacional de Referência para a Cibersegurança (QNRCS) identifica um conjunto de recomendações com vista à implementação de medidas de Identificação, Proteção, Deteção, Resposta e Recuperação contra ameaças que colocam em causa a cibersegurança da organização, envolvendo toda a sua estrutura e tendo em consideração os aspetos humanos, tecnológicos e processuais.

A ISO/IEC 31000 disponibiliza um conjunto de princípios e de orientações genéricas sobre gestão dos riscos para o **Grupo CAC**. Por outro lado, a ISO/IEC 27005 especifica orientações e processos para gestão dos riscos de segurança dos sistemas de informação.

Gestão dos Riscos

A gestão dos riscos do **Grupo CAC** é entendida como a gestão do efeito da incerteza nos objetivos organizacionais e determinação das ações necessárias, para que esses efeitos (probabilidade e consequência) possam ser minimizados para níveis considerados aceitáveis por parte do **Grupo CAC**. Neste sentido, importa introduzir e/ou reforçar alguns conceitos importantes relacionados com a gestão dos riscos:

-Ameaça: Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.

- Vulnerabilidade: Fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.

- Impacto: Prende-se com o resultado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos, evento este que se traduz normalmente em consequências diretas ou indiretas, para os recursos mencionados.

- Risco: Uma circunstância ou um evento razoavelmente identificável, com um efeito potencial adverso na segurança das redes e dos sistemas de informação.

O processo de gestão dos riscos é um exercício estruturado, no qual a organização identifica possíveis ameaças que possam explorar as vulnerabilidades dos ativos, bem como quais os níveis do risco associado, avaliando-se a probabilidade de ocorrência e possíveis impactos.

O tratamento de riscos, consiste nas seguintes etapas:

- Identificação dos riscos (etapa 1);

-Análise dos riscos (etapa 2);

-Avaliação dos riscos (etapa 3);

Durante as etapas do tratamento de riscos, são identificadas as ameaças e vulnerabilidades existentes (ou que possam vir a ser exploradas), identificados os controlos e os efeitos no risco identificado, assim como as consequências ou impactos possíveis e a prioridade.

A prioridade dos riscos é classificada de acordo com o nível do risco que lhe seja atribuído (ver tabelas infra).

Nível do Risco	
1 a 5	Muito Baixo, Desprezível, Mínimo, sem efeito.
6 a 10	Baixo, Menor, Limitado, Circunscrito.
11 a 15	Médio, Moderado, Sério.
16 a 20	Alto, Severo.
21 a 25	Muito Alto, Crítico, Urgente, Catastrófico, Letal.

Critérios de Análise de Riscos		
Riscos	**Probabilidade**	**Impacto (verificar de acordo com os critérios de aferição de impacto)**
Muito Alto (5)	Evento tem ocorrido frequentemente. Há registo de várias ocorrências e é provável que venha a ocorrer novamente num intervalo igual ou inferior a 1 ano.	Evento que gera impacto sobre toda a organização ou representa perda de disponibilidade, confidencialidade e/ou integridade causando prejuízos de forma generalizada, inviabilizando todas as funções primárias ou proporcionando perceção negativa
Alto (4)	Evento tem ocorrido frequentemente. Há registo de mais de uma ocorrência e é provável que venha a ocorrer novamente num intervalo de 1 ano.	Evento que gera impacto sobre vários grupos ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho de múltiplas áreas da organização.
Médio (3)	Evento tem ocorrido, porém não frequentemente. Há registos de uma ocorrência no intervalo de 1 ano.	Evento que gera impacto sobre um grupo relevante ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho.
Baixo (2)	Evento já ocorreu nesse tipo de atividade e é possível que venha a ocorrer novamente no intervalo de 1 ano ou superior	Evento que gera impacto sobre um pequeno grupo ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções secundárias de trabalho, não sendo bastante para intervir nas funções principais.
Muito Baixo (1)	Evento nunca ocorreu nesse tipo de atividade e é altamente improvável que venha a ocorrer num intervalo superior a 3 anos.	Evento que gera impacto sobre apenas uma pessoa ou representa perda de disponibilidade, confidencialidade e/ou integridade que não necessita de intervenção ou paralisação imediata.

Matriz de Riscos					
(5) Muito Alto	Médio (5)	Médio (10)	Alto (15)	Muito Alto (20)	Muito Alto (25)
(4) Alto	Baixo (4)	Médio (8)	Alto (12)	Alto (16)	Muito Alto (20)
(3) Médio	Baixo (3)	Médio (6)	Médio (9)	Alto (12)	Alto (15)
(2) Baixo	Baixo (3)	Baixo (4)	Médio (6)	Médio (8)	Médio (10)
(1) Muito Baixo	Muito Baixo (1)	Baixo (2)	Baixo (3)	Baixo (4)	Médio (5)

Valor do risco e respetivo tratamento	
Descrição	Tratamento Recomendado
Muito Baixo	Aceitar - O risco não é objeto de nenhuma ação, dado que o risco inerente ou residual atende aos critérios de aceitação de risco definidos ao estabelecer o contexto de risco.
Baixo	Aceitar - O risco não é objeto de nenhuma ação, dado que o risco inerente ou residual atende aos critérios de aceitação de risco definidos ao estabelecer o contexto de risco.
	Mitigar - O risco é mitigado através de controlos, políticas, procedimentos ou quaisquer outras medidas adotadas
	Transferir - O risco é transferido para uma terceira entidade.
Médio	Mitigar - O risco é mitigado através de controlos, políticas, procedimentos ou quaisquer outras medidas adotadas.
	Transferir - O risco é transferido para uma terceira entidade.
Alto	Mitigar - O risco é mitigado através de controlos, políticas, procedimentos ou quaisquer outras medidas adotadas.
	Transferir - O risco é transferido para uma terceira entidade.
Muito Alto	Evitar - Parar a atividade que é muito arriscada, ou realizar de modo diferente.
	Mitigar - O risco é mitigado através de controlos, políticas, procedimentos ou quaisquer outras medidas adotadas.

Análise de riscos de corrupção e infrações conexas Organização

A tabela seguinte procura elencar os riscos relevantes da organização, elencando a sua probabilidade e impacto, o nível de risco associado e as medidas preventivas e corretivas que permitem reduzir a sua probabilidade de ocorrência.

Área de Risco	Atividades desenvolvidas	Riscos associados	Impacto	Probabilidade	Nível de risco	Mecanismos de prevenção e/ou mitigação	Estado	Nível Residual
Aquisição de Bens e Serviços	Gestão de processos de aquisição de bens e serviços e controlo de qualidade dos serviços prestados	Favorecimento de fornecedores de bens/serviços com o objetivo de retirar benefícios próprios ou para terceiros.	3	2	6	Código de Conduta; Aquisições obriga sempre a assinatura do Administrador. Controlo da despesa pelo departamento Financeiro; Política de Denúncias Internas; Política de Combate à Corrupção; Certificação 9001 e boas praticas na ótica da qualidade; Atualização regular da base de fornecedores; Acordos de Subcontratação; Controlo de qualidade dos serviços prestados; Auditorias regulares por entidades externas; Sistema de controlo de stocks; Processo de auditorias a fornecedores; Implementação de canal de denúncia.	Mitigado	Baixo
		Divulgação de informação confidencial	3	2	6		Mitigado	Baixo
		Aquisição ou desvio de bens para proveito próprio ou de terceiro	3	2	6			Baixo
	Aquisições	Corrupção ativa ou passiva	2	2	4	Código de Conduta; Procedimentos para Aquisição de Bens/Serviços; Procedimentos de controlo interno, através do ERP; Acordos de Subcontratação; Revisão regular dos procedimentos; Implementação de canais de denúncia. Política de Denúncias Internas Política de Combate à Corrupção	Mitigado	Muito Baixo
		Participação económica em negócio	2	2	4			Muito Baixo
	Verificação de conformidade dos fornecimentos de bens e serviços	Desvio de quantidades e/ou da qualidade dos bens/serviços contratados; Retenção de material por colaborador; Abuso de poder;	2	2	4	Código de Conduta; Informação e sensibilização dos colaboradores; Procedimentos de controlo interno; Acordos de Subcontratação; Certificação ISF Food; Certificação 9001 e boas praticas na ótica da qualidade; Auditorias regulares por entidades externas;	Mitigado	Muito Baixo

Área de Risco	Atividades desenvolvidas	Riscos associados	Impacto	Probabilidade	Nível de risco	Mecanismos de prevenção e/ou mitigação	Estado	Nível Residual
		Tráfico de influência				Implementação de canal de denúncias interno; Política de Denúncias Internas; Política de Combate à Corrupção; Etiquetas de produtos automatizadas; Sistema de controlo de stocks.		
		Contrafação	2	2	4		Mitigado	Muito Baixo
Faturação de bens/serviços	Faturação de bens/serviços	Não registo de serviço prestado; Corrupção ativa ou passiva; Branqueamento de capitais; Desvio de fundos; Evasão fiscal	3	2	6	Código de Conduta; Registo de horas de colaborador despendidas em cliente; Reforço das medidas de controlo interno numa perspetiva de prevenção da corrupção e infrações conexas; Medidas de informação e sensibilização dos colaboradores para as consequências da corrupção e infrações conexa; Política Combate à Corrupção Programa de auditorias internas e externas; Implementação de canal de denúncias interno Política de Denúncias Internas ROC externo	Mitigado	Baixo
	Controlo de faturação	Não registo de serviço prestado; Corrupção ativa ou passiva; Branqueamento de capitais; Desvio de fundos; Evasão fiscal	3	2	6		Mitigado	Baixo
	Falha/avaria do sistema informático	Recebimento de valores sem emissão de documento de quitação pelo sistema informático	2	2	4	Código de conduta; Sistema ERP e logs do Sistema; Políticas internas do Sistema de Gestão; Reforço das medidas de controlo interno numa perspetiva de prevenção da corrupção e infrações conexas.	Mitigado	Muito Baixo

Área de Risco	Atividades desenvolvidas	Riscos associados	Impacto	Probabilidade	Nível de risco	Mecanismos de prevenção e/ou mitigação	Estado	Nível Residual
Administração	Processo decisório em todas as matérias da Organização	Desvirtuação do processo decisório da Organização; Entraves à transparência; Tráfico de influência; Apropriação ou utilização indevida de bens imóveis ou móveis Organização, designadamente para fins privados.	3	2	6	Código de Conduta; Reuniões de Administração com a participação dos vários Administradores, com transcrição em ATA; Publicação da ATA em Repositório interno; Formação e sensibilização a colaboradores e dirigentes; Procedimentos de controlo interno; Controlo e aprovação das contas pelo Departamento Financeiro Reforço das medidas de controlo interno numa perspetiva de prevenção da corrupção e infrações conexas; Auditorias internas e externas aos reportes financeiros; Implementação de canal de denúncias interno. Política de Denúncias Internas	Mitigado	Baixo
Gestão financeira	Controlo Orçamental	Adulteração e/ou omissão de informação que condicione a representação, de forma verídica e transparente, da situação financeira; Desvio de subsídio; Desvio de valores; Branqueamento de capitais;	3	2	5	Código de Conduta; Formação e sensibilização a colaboradores e dirigentes; Procedimentos de controlo interno; Gestão de Acessos; Vários níveis de validação de informação; Controlo e aprovação pelo Departamento Financeiro; Política Combate à Corrupção; Auditorias internas e externas aos reportes financeiros; Reforço das medidas de controlo interno numa perspetiva de prevenção da corrupção e infrações conexas; Implementação de canal de denúncias interno. Política de Denúncias Internas; ROC externo	Mitigado	Muito Baixo
	Gestão Contabilística	Branqueamento de capitais.						
Recursos Humanos	Processo de recrutamento e seleção	Critérios de recrutamento e seleção ambíguos	2	2	4	Código de Conduta; Política Combate à Corrupção; Política de Denúncias Internas; Vaga aberta com identificação dos critérios, Processo de recrutamento em várias fases, dependendo das áreas; Participação de diversos intervenientes no processo de recrutamento, dependendo das áreas; Implementação de canal de denúncias interno.	Mitigado	Muito Baixo
		Favorecimento ilícito na escolha dos recursos humanos a recrutar	2	2	4		Mitigado	Muito Baixo

Área de Risco	Atividades desenvolvidas	Riscos associados	Impacto	Probabilidade	Nível de risco	Mecanismos de prevenção e/ou mitigação	Estado	Nível Residual
	Formação profissional	Falsificação de documentos de formação	3	2	6	Elaboração de Plano Anual de Formação com base nas iniciativas propostas pelas diversas áreas de negócio atendendo às necessidades internas; Possibilidade de o próprio colaborador sugerir formações necessárias ou almejadas; Controlo, acompanhamento e avaliação das ações de formação realizadas; Cláusulas de confidencialidade nos CT, com inclusão de regras de utilização de recursos; Formações contratadas a entidades externas; Implementação de canal de denúncias interno. Política de Denúncias Internas	Mitigado	Baixo
	Processamento de remunerações, abonos, descontos e processos individuais dos colaboradores	Manipulação da informação de modo a facilitar o pagamento indevido de benefícios e compensações; Risco de acesso impróprio às informações pessoais / quebra de sigilo; Risco de falhas no registo da informação das bases de dados pessoais; Evasão fiscal.	3	2	6	Código de Conduta; Política de Combate à Corrupção; Política de Denúncias Internas; Gestão de Acessos; Registo de horas extras através de pedido Controlo de Absentismo através de sistema biométrico Regulamento Geral de Proteção de Dados; Controlo de entradas e saídas automático; Formação e sensibilização a dirigentes e colaboradores sobre os riscos de corrupção; Formação e sensibilização dos colaborados em matéria de proteção de dados; Cláusulas de confidencialidade nos CT, com inclusão de regras de utilização de recursos; Intervenção de mais do que um interlocutor no âmbito do processamento de remunerações, abonos e descontos; Controlo por departamento Financeiro; Plano de auditorias internas e externas; Implementação de canal de denúncias interno. Política de Denúncias Internas ROC	Mitigado	Baixo

Área de Risco	Atividades desenvolvidas	Riscos associados	Impacto	Probabilidade	Nível de risco	Mecanismos de prevenção e/ou mitigação	Estado	Nível Residual
Sistema de Informação	Segurança dos Sistemas de Informação; Gestão de programas e aplicações informáticas; Identificação e Autenticação de usuários; Autorização e controlo de acessos; Registos de Auditoria nos programas e aplicações	Falhas de cumprimento de Procedimentos internos de segurança em benefício próprio ou de terceiros; Uso indevido das bases de dados e informação em geral; Corrupção passiva para ato ilícito; Falhas dos colaboradores da área de sistemas de informação em benefício do próprio e de terceiros.	3	2	6	Código de Conduta; Monitorização contínua da segurança da Informação; Formação e sensibilização a colaboradores; Cláusulas de confidencialidade nos CT, com inclusão de regras de utilização de recursos; Perfis de acesso; Cláusula de confidencialidade após a saída dos colaboradores; Implementação de canal de denúncias interno. Política de Denúncias Internas	Mitigado	Baixo
Jurídico	Assessoria jurídica	Divulgação de informação confidencial	2	2	4	Descentralização da área jurídica para prestadores de serviços;	Mitigado	Muito Baixo
	Contencioso	Divulgação de informação confidencial; Corrupção ativa ou passiva; Tráfico de influência	2	2	4	Descentralização da área jurídica para prestadores de serviços;	Mitigado	Muito Baixo

Publicidade e Revisão do Plano

O presente Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, entra em vigor, no dia útil seguinte à sua publicação, devendo ser objeto de uma avaliação anual. Para tal, é competente o Responsável do Cumprimento Normativo que procede ao controlo periódico no sentido de verificar se está a ser assegurado o cumprimento das regras do Plano e os seus efeitos práticos.

O PPR deverá ser revisto a cada três anos, ou sempre que se opere uma alteração significativa nas atribuições, estrutura societária que justifique a revisão do PPR. Independentemente da periodicidade das revisões e atualizações, sempre que surjam riscos que importe prevenir, devem os responsáveis informar o Responsável do Cumprimento Normativo.

A divulgação do presente PPR, bem como dos relatórios previstos no ponto Acompanhamento, Avaliação e Monitorização do PPR, é feita a todos os seus colaboradores e parceiros, através de publicação interna, e da disponibilização no seu site em https://www.grupocac.pt/.

É da responsabilidade da Administração e de todos os colaboradores, assegurar o cumprimento das regras do presente Plano.

Data: 14/08/2025