

Relatório Anual de Execução Plano de Gestão de Riscos de Corrupção e Infrações Conexas 2017

ÍNDICE

1. Introdução.....	4
2. Execução do PGRIC de 2017.....	4
3. Avaliação das medidas de controlo.....	5
4. Medidas de Controlo Planeadas.....	6
Anexo I.....	8

SIGLAS

CISO	Coordenador de Segurança de Informação
CPC	Conselho Prevenção da Corrupção
CRO	<i>Chief Risk Officer</i>
DAI	Direção de Auditoria Interna
DCM	Direção Comercial e Marketing
DCP	Direção de Compras
DFI	Direção Financeira
DJU	Direção de Serviços Jurídicos
DME	Direção de Manutenção e Engenharia
DPC	Direção de Planeamento e Controlo de Gestão
DPI	Direção de Programas e Investimentos
DRH	Direção de Recursos Humanos
DSA	Direção de Segurança e Apoio Geral
DSI	Direção de Sistemas de Informação
INCM	Imprensa Nacional – Casa da Moeda, SA
ISO	<i>International Organization for Standardization</i>
NP	Norma Portuguesa
PGRCIC	Plano de Gestão de Riscos de Corrupção e Infrações Conexas
SLG	Serviço de Logística
SLI	Serviço de Laboratório Industrial
UCO	Unidade de Contrastaria
UGF	Unidade Gráfica
UMD	Unidade de Moeda
UPB	Unidade de Publicações

1. INTRODUÇÃO

As Recomendações que o Conselho de Prevenção da Corrupção (CPC) tem emitido desde 2009, sendo a mais recente de 4 de maio de 2017, incidem sobre a necessidade dos dirigentes máximos das entidades gestoras de dinheiro, valores e património públicos, adotarem e divulgarem Planos de Gestão de Riscos de Corrupção e Infrações Conexas (PGRIC).

Nestes Planos, devem ser identificados de modo exaustivo os riscos de corrupção e infrações conexas de forma a planear um conjunto de medidas que permitam melhorar a prevenção da corrupção e infrações conexas. As medidas reconhecidas, devem obrigatoriamente identificar um responsável pela execução das ações planeadas e por assegurar que as mesmas mitigam efetivamente os respetivos riscos.

Assim, embora a responsabilidade da identificação dos riscos seja dos gestores dos respetivos processos da INCM, estes devem identificar nominalmente os donos do risco. Adicionalmente, cabe ao CRO a monitorização holística de todo o registo de riscos e à DAI a avaliação do processo de gestão de risco. O Comité de Gestão de Riscos Corporativos avalia periodicamente o estado da gestão de riscos com base nos contributos dos responsáveis aqui identificados.

O presente relatório descreve o acompanhamento realizado ao PGRIC de 2017, o estado atual, e identifica as principais medidas a adotar de acordo com o PGRIC de 2018. Note-se que as responsabilidades e controlos internos da gestão de riscos são detalhados no Plano que pode ser consultado em:

https://www.incm.pt/portal/incm_gr.jsp.

2. EXECUÇÃO DO PGRIC DE 2017

Em 2017, o Comité de Gestão de Riscos Corporativos aprovou a implementação de uma *Framework* de Gestão de Riscos Corporativos que define o conjunto de elementos que fornecem os fundamentos e disposições organizacionais, para conceber, implementar, monitorizar, rever e melhorar continuamente a gestão do risco na INCM.

A *Framework* adotada vem alinhar a INCM com as melhores práticas nestas matérias e garantir que os requisitos internos e externos são cumpridos. Nesse sentido, a *Framework* definida encontra-se alinhada com as normas ISO31000:2009, ISO/IEC31010:2009, e ISO *Guide* 73:2009. O objetivo foi assegurar que a INCM possui uma *Framework* transversal à organização que permite evitar a criação de silos e conseqüente duplicação de esforços.

Em conseqüência dessa ação a INCM procedeu à revisão da informação de risco com vista a assegurar:

- Uma melhor descrição dos riscos através da introdução no processo de gestão de riscos dos conceitos de causa e conseqüência;
- Reavaliar os riscos existentes com base nas novas descrições de risco;

- Identificar novos riscos revendo os atuais processos de negócio e apoio da organização;
- Assegurar uma melhor análise dos riscos através da introdução dos conceitos de probabilidade, impacto e nível de risco;
- Uma descrição mais fina dos controlos substituindo controlos genéricos por ações específicas e de natureza prática.

Adicionalmente, de forma a garantir a eficiente monitorização e comunicação dos riscos através da introdução de relatórios de risco produzidos pelo CRO, função estabelecida em 2017, responsável pela implementação das atividades de Gestão de Risco Corporativo em estreita colaboração com as diversas unidades orgânicas da INCM, assegurando uma constante identificação, análise e avaliação dos riscos da organização.

A última revisão da informação de risco foi efetuada em fevereiro de 2018 e incluiu os processos de negócio e apoio reproduzidos no Anexo I. A revisão permitiu, em relação ao PGRCIC de 2017:

- Identificar novos riscos de corrupção e infrações conexas;
- Identificar novas medidas de prevenção da corrupção e infrações conexas;
- Melhorar a identificação, análise e avaliação dos riscos existentes;
- Integrar riscos redundantes ou semelhantes;
- Eliminar riscos com informação considerada deficiente, ou resultantes de causas que não podem mais ocorrer devido a alterações de processo ou atividade.

Dadas as significantes alterações ao modelo de domínio, o presente relatório não identifica todas as mudanças realizadas ao anterior plano dando ênfase às medidas acompanhadas durante o ano e as medidas planeadas para 2018.

3. AVALIAÇÃO DAS MEDIDAS DE CONTROLO

Os controlos definidos no plano de gestão de riscos de corrupção e infrações conexas de 2017 encontram-se implementados considerando-se que reforçam o sistema de controlo interno face aos riscos identificados. Durante o ano de 2017 destaca-se a definição dos seguintes processos:

- Processo de Apoio - Project Management Office
- Processo de Apoio - Gestão de Riscos Corporativos;
- Processo de Apoio - Direção Financeira

Relativamente às medidas referidas no PGRCIC de 2017 as mesmas foram incluídas nos objetivos das unidades orgânicas e monitorizadas pela Direção de Planeamento e Controlo de Gestão, com os seguintes resultados. As medidas que não foram concluídas transitam para o ano de 2018.

Medida	Situação a 31-03-2018
1. Fomentar uma cultura de gestão de risco	● concluída
2. Regulamento de proteção de dados	● em curso
3. Definição de um modelo de <i>governance</i> de segurança de informação	● em curso
4. Ações de sensibilização aos monitores e auditores	● concluída
5. Melhoria dos procedimentos e processos da DAI	● concluída

Relativo ao plano de formação, no ano de 2017 foram promovidas ações com vista a uma maior sensibilização de todos os colaboradores para a necessidade de mitigar ou eliminar o risco de práticas de corrupção e conflitos de interesses, destacando-se:

- Ações de formação sobre a ISO22301 -gestão de risco e continuidade de negócio;
- Ações de formação sobre as transições das normas ISO9001 e ISO14001 que destaca as ações de gestão de risco como processos fundamentais na gestão das organizações;
- Formação E-learning no âmbito da Gestão da Segurança da Informação (ISO27001);
- Formação On Job, realizadas pelo CISO, a entidades externas subcontratadas no âmbito da Gestão da Segurança da Informação (ISO27001);
- Formação On Job, realizadas pelo CRO, no âmbito da implementação da nova Framework de Gestão de Risco Corporativo;
- Outras ações de formação/participação em conferências relativas à Gestão de Riscos.

Importante ainda informar que durante o ano de 2017 o Comité de Ética recebeu uma participação interna relativa a ofertas a colaboradores que foi tratada e dada como concluída.

4. MEDIDAS DE CONTROLO PLANEADAS

Atendendo aos riscos identificados no PGRCIC de 2018 (que pode ser consultado em https://www.incm.pt/portal/incm_gr.jsp) concluiu-se que, com as medidas de tratamento de risco implementadas, o risco de corrupção e infrações conexas na INCM é “muito baixo” não havendo pontos fracos relevantes a melhorar. Não obstante o nível de risco apresentado estabelece-se as seguintes medidas para 2018 de forma a reforçar o combate à prevenção da corrupção e infrações conexas.

Medida	Riscos Relacionados ¹	Dono do Risco
Melhoria dos registos e <i>audit log</i> de acesso remoto	R14	DSI
Implementação de sistema de autenticação de utilizador que faz pedido de nova <i>password</i>	R16	DSI
Controlo, via <i>Firewall</i> , dos acessos e seleção de nova aplicação de suporte remoto	R18	DSI
Implementação de um sistema online para receber dados do cliente	R38	DCM
Introdução de controlos de acesso à Divisão Comercial da Gráfica da DCM	R39	DCM
Implementação de deteção de metais	R42	DSA
Renovação do parque IT das máquinas de produção a cargo da DME	R53	DME
Definição e revisão de procedimento de venda de equipamento produtivo	R54	DSA
Colocação de sistema de CCTV e controlo de acesso restrito em novas zonas	R56-57; R62-67	DSA
Implementação de plano de formação/aptidão, treino e rotatividade na produção	R60	UGF
Classificação de Matérias-Primas e Produtos Gráficos de Segurança	R62-63; R65-67	UGF
Criação de sala de destruição junto ao armazém de Controlo Produtos Gráficos (CPG) na cave	R62; R66-67	UGF
Utilização de sistema SAP para controlo de punções	R78; R79	UCO

Para além das medidas referidas a organização irá prosseguir com a realização de auditorias internas às áreas e processos onde foram identificados os riscos mais severos de corrupção e conflitos de interesses, e na promoção de ações de formação que permitam sensibilizar os colaboradores para o tema da prevenção da corrupção.

¹ Os riscos aqui mencionados podem ser consultados no Plano de Corrupção e Infrações Conexas de 2018 em https://www.incm.pt/portal/incm_gr.jsp

ANEXO I

Tabela 1. Processos de Negócio

ID	Descrição	Responsável
PN 01	Comercialização Produtos Gráficos	DCM
PN 02	Divisão Comercial da Moeda	DCM
PN 03	Produção de Moeda e Produtos Metálicos	UMD
PN 04	Fabrico de Produtos Gráficos	UGF
PN 05	Conceção e Desenvolvimento dos Produtos Gráficos e Produtos Metálicos	DCM
PN 07	Publicações Oficiais	UPB
PN 08	Lojas e Distribuição	DCM
PN 09	Edição de Livros	UPB
PN 11	Unidade das Contrastarias	UCO

Tabela 2. Processos de Apoio

ID	Descrição	Responsável
PA 01	Recursos Humanos	DRH
PA 02	Compras	DCP
PA 03	Manutenção de Equipamentos e Infraestruturas Fabris	DME
PA 04	Gestão de Equipamentos de Monitorização e Medição	SLI
PA 05	Implementação e Manutenção de Sistemas e Aplicações	DSI
PA 06	Logística	SLG
PA 07	Segurança Física	DSA
PA 08	Regras de Segurança Informática	DSI
PA 09	Auditoria Interna	DAI
PA 10	Gestão dos Riscos de Segurança da Informação	CISO
PA 11	Comercial e Marketing	DCM
PA 12	Direção dos Serviços Jurídicos	DJU
PA 13	Planeamento e Controlo de Gestão	DPC
PA 14	Obras e Contratos de Manutenção	DSA
PA 15	Serviços Gerais	DSA
PA 16	Segurança da Informação	CISO
PA 17	<i>Project Management Office</i>	DPI
PA 18	Gestão de Riscos Corporativos	DPC
PA 19	Direção Financeira	DFI