TÉCNICO LISBOA

Modelo de Informação de Referência para Gestão de Risco no Contexto de Corrupção e Infrações Conexas

Filipe Miguel da Cunha Semanas

Dissertação para obtenção do Grau de Mestre em

Engenharia e Gestão Industrial

Orientador: Prof. José Luís Brinquete Borbinha

Júri

Presidente: Prof. José Rui de Matos Figueira
Orientador: Prof. José Luís Brinquete Borbinha
Vogal: Prof.ª Maria do Rosário Gomes Osório Bernardo Ponces de Carvalho

Novembro 2016

Resumo

Em 2009, o Conselho de Prevenção da Corrupção (**CPC**) requisitou a todas as organizações que estivessem envolvidas na “gestão e administração de dinheiros, valores ou património públicos” [1] que elaborassem planos de gestão de risco para o contexto da corrupção e infrações conexas.

Ao longo dos cinco anos que se seguiram à recomendação em [1], o **CPC** conduziu uma análise sobre a implementação desses planos nas várias organizações. Concluiu-se que estes são uma ferramenta útil no combate à corrupção. No entanto, verificou-se também uma heterogeneidade significativa entre os vários planos; em apenas uma pequena percentagem dos mesmos era evidente a aplicação de qualquer método formal. [2]

Reveste-se assim de particular interesse a existência de um modelo de referência para a gestão de risco. Sendo assim, o seguinte trabalho tem como finalidade sugerir um modelo de informação de referência para a gestão de riscos no âmbito da corrupção e infrações conexas. Para validação do modelo recomendado, procedeu-se à aplicação do mesmo para dados reais de organizações de três áreas distintas: **INCM** (área de produção de bens/serviços para o Estado), **IST** (área de educação/investigação), e **LNEC** (área de I&D para engenharia civil).

Concluiu-se que o modelo resultante deste trabalho pode ser uma mais-valia na prevenção da corrupção e de infrações conexas em qualquer organização. Mais, sendo este um modelo de referência, garante-se uma maior homogeneidade entre os planos de gestão de riscos das várias organizações nacionais.

Palavras-Chave: Gestão de Riscos, Corrupção, Modelo de Informação, Método Indutivo, Registo de Riscos, ISO 31000

Abstract

In 2009, *Conselho de Prevenção da Corrupção* (**CPC**) requested the conception of a risk management plan for corruption to all organizations somehow involved in the management of public assets. [1]

In the five years that followed such recommendation, **CPC** conducted an analysis about the implementation of those plans over the targeted organizations. It was concluded that those plans are useful tools in preventing corruption. However, it was also noticeable a significant heterogeneity among all those risk management plans; as in only a small percentage of said plans, it was utilized any perceived formal methodology. [2]

Hence, the relevance of a reference model for risk management and, therefore, for this project. In it, it is suggested a reference risk management framework for corruption and, in order to validate the recommended model, the model was applied to real-life cases related to organizations in three distinct fields of work: **INCM** (production of goods/services to the Portuguese State), **IST** (Education and Scientific Research), and **LNEC** (I&D related to civil engineering).

It was concluded that the resulting framework can indeed provide added value to any organization's attempts in preventing corruption. Moreover, this is intended to be a reference framework, which means it would ensure a greater homogeneity among the risk management plans of the various Portuguese organizations.

Keywords: Risk Management, Corruption, Framework, Inductive Reasoning, Risk Register, ISO 31000

Agradecimentos

Em primeiro lugar, quero agradecer ao profº José Borbinha e Ricardo Vieira pelo apoio, orientação e disponibilidade que apresentaram para comigo no contexto da elaboração desta dissertação. Acima de tudo agradeço a paciência que tiveram mediante as dificuldades (e os "devaneios artísticos") com que me deparei ao longo deste período. Uma nota especial também para o Carlos Martins que me ajudou a implementar alguns dos meus resultados na *HoliRisk* e para o profº Leonardo Gonçalves que desde muito cedo demonstrou um grande interesse pelo trabalho que estava a desenvolver.

Em segundo lugar, mas não por ser de menor importância, deixo o agradecimento à minha família tanto pelo carinho com que sempre me trataram assim como pela estabilidade que me deram para a realização deste trabalho a custo de vários sacrifícios pessoais; especialmente os meus pais (e uma menção para o meu avô que falta faz mesmo após estes anos). Também sinto que devo agradecer aos meus amigos mais próximos pelo apoio que também me deram (cada um à sua maneira).

Por último, queria fazer uma menção geral a todas as pessoas que me foram possibilitando adquirir o conhecimento académico que pretendo aplicar nesta dissertação; conhecimento que foi assimilado ao longo de dezassete anos, não só no Instituto Superior Técnico, mas também em Odivelas, particularmente na Escola Secundária da Ramada (onde passei os três melhores anos da minha vida) e na Escola Básica Isabel de Portugal.

"E quando você quer alguma coisa,
todo o Universo conspira para que
você realize seu desejo."

Paulo Coelho

Índice

Índice de Figuras

Lista de Acrónimos

ACFE – Association of **C**ertified **F**raud **E**xaminers
CPC – **C**onselho de **P**revenção da **C**orrupção
DIS – **D**raft **I**nternational **S**tandard
ERM – **E**nterprise **R**isk **M**anagement
EU – **E**uropean **U**nion
INCM – **I**mprensa **N**acional – **C**asa da **M**oeda
ISO – **I**nternational **O**rganization for **S**tandardization
IST – **I**nstituto **S**uperior **T**écnico
LNEC – **L**aboratório **N**acional de **E**ngenharia **C**ivil
PDCA – **P**lan; **D**o; **C**heck; **A**ct
PGRCIC – **P**lano de **G**estão de **R**iscos de **C**orrupção e **I**nfrações **C**onexas
StAR – **St**olen **A**sset **R**ecovery Initiative
UN – **U**nited **N**ations
UNCAC – **U**nited **N**ations **C**onvention **a**gainst **C**orruption

1. Introdução

O presente capítulo tem o objetivo de introduzir o leitor ao conteúdo deste documento. Começar-se-á com uma contextualização do problema deste trabalho, à qual se seguirá a listagem dos objetivos do mesmo.

De seguida explicar-se-á, o mais sucintamente possível, o método utilizado ao longo deste trabalho e, para concluir esta introdução, mostrar-se-á como se encontra estruturado o resto deste documento.

1.1 Contextualização do Problema

Segundo o *Conselho de Prevenção da Corrupção* (**CPC**), "a atividade de gestão e administração de dinheiros, valores e património públicos, seja qual for a natureza da entidade gestora (…) deve, nos termos da Constituição da República e da lei, pautar-se por princípios de interesse geral, nomeadamente, da prossecução do interesse público, da igualdade, da proporcionalidade, da transparência, da justiça, da imparcialidade, da boa-fé e da boa administração" [1].

Ora, tendo em conta que "o fenómeno da corrupção constitui uma violação clara de tais princípios" [1], o **CPC** decidiu aprovar uma recomendação, emitida no dia 1 de julho de 2009, que requisitava a elaboração de planos de gestão de risco a todas as organizações pertencentes ao domínio anteriormente mencionado. Esses documentos seriam os *Planos de Gestão de Riscos de Corrupção e Infrações Conexas* (**PGRCIC**) e, neles, o **CPC** pretendia que fossem identificados possíveis riscos de corrupção e que fossem definidas medidas para prevenir tais riscos. [1]

No dia 15 de junho de 2015, o **CPC** apresentou um balanço do desenvolvimento desses **PGRCIC**'s no período entre 2009 e 2014. De acordo com esse documento, no final de 2014, cerca de mil organizações já tinham seguido a recomendação da **CPC**, tendo então concebido planos de gestão de risco no âmbito da corrupção e infrações conexas. Mais, esse estudo do **CPC** durante esse período confirmou a utilidade desses planos como ferramentas para uma melhor gestão pública.

Todavia, também foi possível inferir que os planos de gestão de riscos concebidos são muito heterogéneos; isto é, são utilizados modelos de domínio distintos em cada empresa. Mais; na maior parte desses documentos, não é percetível que tenha sido seguido qualquer método formal por parte da respetiva organização. Com efeito, somente 41,2% das organizações seguiram uma norma formal na elaboração dos seus respetivos planos de gestão de risco. [2]

1.2 Objetivos

Normas são uma ferramenta de harmonização de processos técnicos e contribuem para facilitar a comunicação numa organização. Estes fornecem: (1) a confiabilidade (o que aumenta a

confiança); (2) apoio às políticas governamentais e legislação; (3) eles fornecem uma base sobre a qual melhorar as práticas existentes ou criar novas. No entanto, como se verificou na subseção **1.1**, a maior parte das organizações no domínio do problema não seguiu qualquer método formal para a elaboração da sua estrutura[1] de gestão de risco.

Assim sendo, o principal objetivo deste trabalho é sugerir um modelo de informação de referência para a gestão de riscos com a temática de corrupção e infrações conexas em mente. Ao basear esse modelo num método formal, espera-se que o resultado deste trabalho possa contribuir para uma maior homogeneidade e uma melhor qualidade global em futuros planos de gestão de risco.

De qualquer maneira, o foco do presente estudo deve ser claramente definido, já que existem frequentemente divergências sobre em que consistem realmente os riscos de "corrupção" e "infrações conexas". Como se pode verificar na **Figura 1**, a *Association of Certified Fraud Examiners* (**ACFE**) considera que corrupção é uma forma de fraude assim como, por exemplo, suborno é uma das várias formas de corrupção. Com base nesse pressuposto, para este trabalho, assume-se que "infrações conexas" refere-se a todas as formas de fraude que não se enquadrem no âmbito de corrupção. Como se pretende auxiliar na elaboração dos planos de gestão de riscos para "corrupção e infrações conexas", vão ser então considerados todos os riscos classificados como "fraude" de acordo com a **Figura 1.**

1.3 Método de Trabalho

Como se pode constatar com o auxílio da **Figura 2**, o método utilizado ao longo deste trabalho tem a finalidade de obter um modelo de referência para a gestão de risco no *silo* da corrupção (e infrações conexas).

A base desse método assenta na revisão da literatura, sendo de esperar que a mesma forneça informação relevante para a conceção de um modelo assente em boas-normas de gestão de risco. Findada essa revisão, procurar-se-á aplicar o conhecimento adquirido a um caso de estudo correspondente a uma das organizações que elaborou um plano de gestão de riscos a pedido do **CPC**; nomeadamente o caso do *Metro Lisboa*. Na análise deste caso, pretendem-se inferir conclusões sobre métodos utilizados na elaboração de um plano de gestão de risco e sobre falhas nos modelos concebidos.

Após essa breve análise, procurar-se-á aplicar a ferramenta *registo de riscos* de acordo com as normas revistas no estado-da-arte, e validar a proposta de solução do problema mediante a aplicação desse modelo a dados reais da **INCM**, **IST** e **LNEC**. Pretende-se, com esse processo, testar a validade do modelo de informação de referência proposto.

[1] *Estrutura* é o termo utilizado na versão portuguesa da norma ISO 31000 para se referir a uma *framework*.

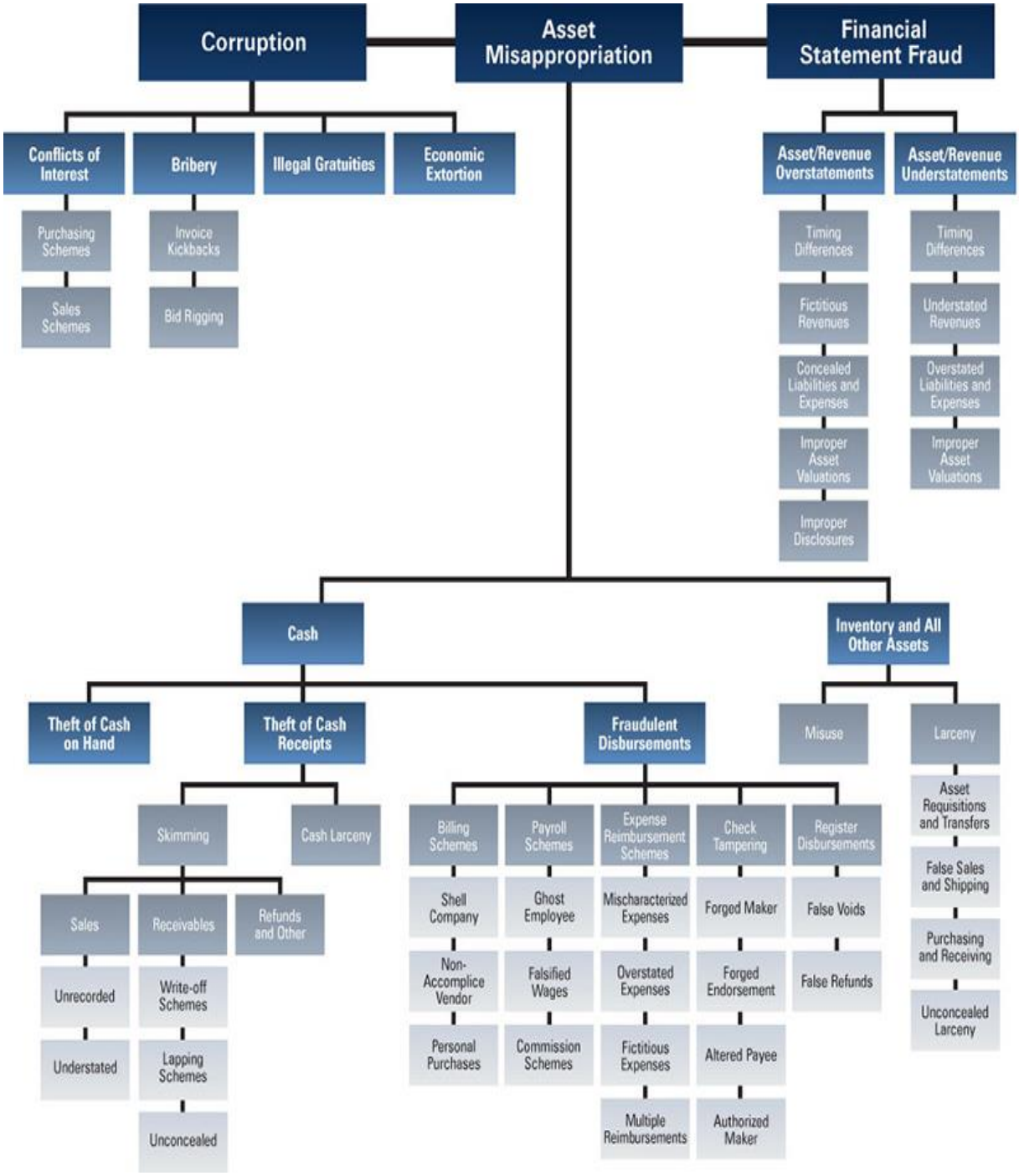

Figura 1 – ACFE Fraud Tree (Fonte: [3])

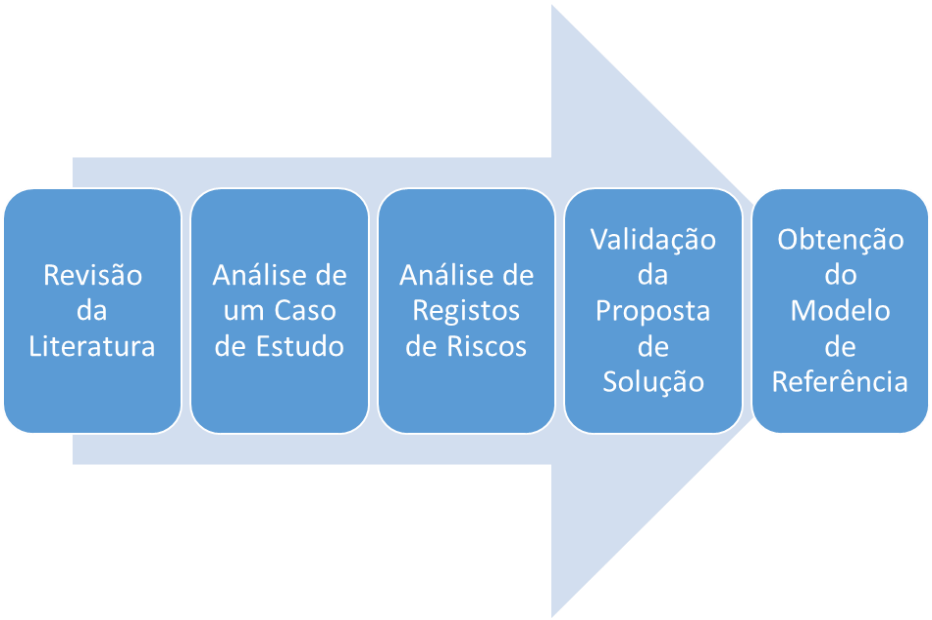

Figura 2 – Método seguido

1.4 Estrutura do Documento

No presente capítulo, realizou-se uma contextualização do problema a estudar neste trabalho, quais os objetivos do mesmo e apresentou-se o método seguido.

No capítulo **2**, será conduzido um levantamento do estado-da-arte na gestão de risco. Será estudada a norma ISO 31000; a sua importância e utilidade para a gestão de risco. Serão também analisados alguns dos principais esforços institucionais de combate à corrupção, o estado da gestão de risco em indústrias distintas e a norma ISO 37001 de combate ao suborno.

Após o levantamento das boas-normas da gestão de risco, pretende-se que, com o capítulo **3**, se encontre uma possível resolução para como configurar/estruturar uma estrutura de informação de gestão de risco no âmbito da corrupção. Analisa-se o problema deste trabalho mediante a ilustração do caso do *Metro Lisboa*; procurar-se-á analisar como é que registos de riscos têm sido utilizados nesses planos de gestão de risco. Por conseguinte, é estudada a possibilidade de aplicar um registo de riscos como solução do problema, sendo que esta ferramenta pode ser utilizada tanto numa folha de *excel* como numa estrutura de informação concebida especificamente para o efeito como é o caso da *HoliRisk*, um *software* atualmente em desenvolvimento pelo INESC-ID. Para concluir o capítulo, demonstra-se que é possível utilizar o modelo de registo de riscos proposto para estruturar dados reais de empresas em indústrias distintas (**INCM, IST** e **LNEC**). Essa aplicação de dados tem como objetivo validar a solução do problema, isto é, garantir que a estrutura de riscos genérica funciona mediante aplicação de casos práticos.

No capítulo **4**, é então apresentado o resultado final do trabalho desenvolvido, assim como uma análise crítica ao mesmo. Nessa discussão, pretendem-se identificar pontos fortes e possíveis

vulnerabilidades da solução, e que valor é acrescentado para organizações que usem esta estrutura de risco.

Por último, no capítulo **5**, conclui-se este relatório com um balanço do que foi o trabalho desenvolvido, da relevância deste trabalho para as organizações no domínio do problema assim como da sua utilidade, e como este trabalho pode ser a base para outros projetos de engenharia no futuro.

2. Revisão da Literatura sobre Gestão de Risco

No presente capítulo, realizar-se-á uma revisão da literatura sobre gestão de risco. Estudar-se-á a norma ISO 31000, assim como dois documentos que a complementam: o ISO Guide 73 e a norma ISO 31010.

Também se procederá a um levantamento dos principais esforços institucionais para combate a riscos de corrupção e/ou conexos, e a um estudo comparativo de fatores catalisadores de corrupção em diferentes indústrias.

Para concluir, será conduzida uma análise à norma ISO 37001 que se encontra em desenvolvimento pela **ISO** e que se espera que seja uma norma para combate ao suborno.

2.1 ISO 31000 – Norma de Princípios e Recomendações para Gestão de Risco

Em novembro de 2009, a **ISO** publicou o documento *ISO 31000: Risk Management – Principles and Guidelines*, que estabelece uma série de princípios que precisam ser satisfeitos a fim de tornar a gestão de riscos mais eficiente. Esse documento foi elaborado com base na norma AS/NZS4360 que foi usada na Austrália e na Nova Zelândia durante quinze anos. Atualmente, a maior parte dos *países desenvolvidos* (incluindo Portugal) já adotou a norma ISO 31000 como a norma nacional oficial para gestão de risco.

A norma ISO 31000 pode ser rapidamente descrita como uma norma *"umbrela"* (ver **Figura 3**[2]) para normas ISO existentes ou futuras referentes à gestão de riscos. Isto significa que, no futuro, a **ISO** poderá conceber normas de gestão de risco mais específicas como se espera ser o caso da norma ISO 37001, específica para o fenómeno do suborno (ver subsecção **2.5**). No entanto, atualmente, a ISO não possui qualquer norma de gestão de risco específica para todo o âmbito da corrupção e infrações conexas.

O benefício mais visível da implementação da norma ISO 31000 é a sua aplicabilidade quer em organizações que já tenham implementado gestão de risco no passado quer em organizações que nunca o tenham feito. Dependendo se (1) gestão do risco nunca foi implementada, (2) foi implementada, mas não de uma forma harmonizada nas diferentes unidades da organização ou (3) foi implementada com sucesso em toda a organização; a norma ISO 31000 pode ser usada como orientação para (1) desenvolver, (2) harmonizar ou (3) identificar pontos fortes e lacunas no sistema de gestão de risco existente.

Quanto à aplicação em negócios, a norma ISO 31000 pode ser usada para criar ou melhorar as estruturas de gestão de risco, processos de gestão de risco ou vocabulário de gestão de risco. Tal já levou algumas associações profissionais a adaptar as suas estruturas de gestão de risco, a fim de atender os requisitos da norma ISO 31000.

[2] Créditos da imagem pertencem a Kulwal, M.

Conforme exibido na **Figura 4**, a norma ISO 31000 considera que a gestão de riscos numa organização seria mais eficaz se se tivesse em consideração a relação existente entre os princípios da norma, a estrutura e o processo. Os princípios da norma ISO 31000 podem ser tomados para construir a fundação de gestão de risco eficaz numa organização. Por sua vez, essa fundação pode ser usada como base para a elaboração da estrutura de gestão de risco na organização. Em seguida, a organização pode avançar para a conceção dos seus processos de gestão de risco. [4]

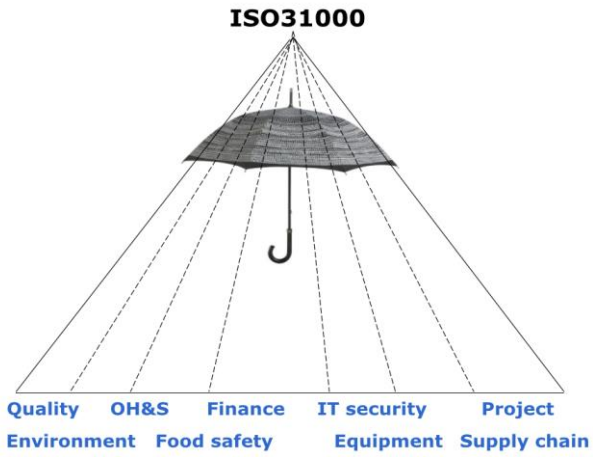

Figura 3 – Aplicação possível de uma norma *"umbrella"* em múltiplas temáticas

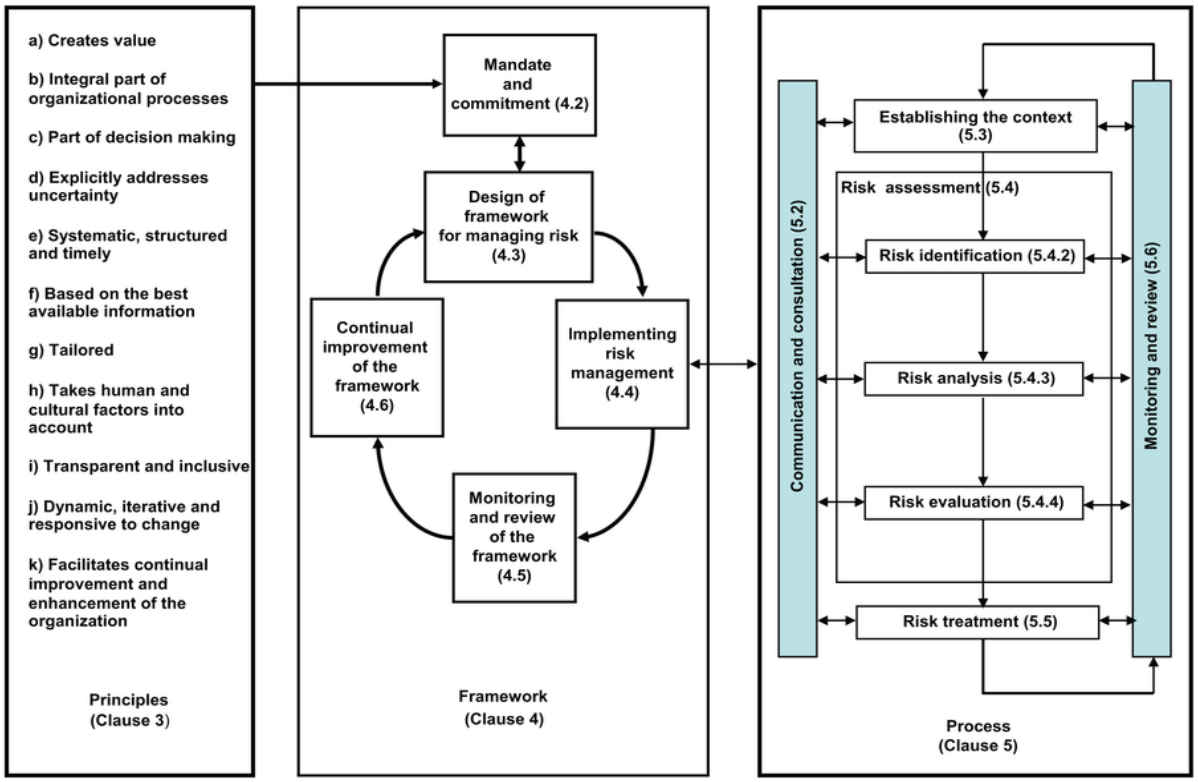

Figura 4 – Relação entre os princípios da norma ISO 31000, estrutura e processo (Fonte: [4])

Nos próximos parágrafos, seguem-se algumas definições essenciais para um bom entendimento de gestão de riscos.

De acordo com [5], *riscos* são o "efeito da incerteza sobre os objetivos"[3], sendo *incerteza* considerada "o estado, mesmo parcial, da deficiência de informações relacionadas com, a compreensão ou o conhecimento de, um evento, sua consequência, ou a probabilidade"[4]. Os riscos podem ter efeitos positivos ou negativos sobre os objetivos do projeto (como, por exemplo, orçamentação e/ou qualidade). Os riscos com efeitos positivos são geralmente denominados de *oportunidades* enquanto os riscos com efeitos negativos são habitualmente descritos como *ameaças*.

Risco é frequentemente caracterizado por referência a *eventos* e *consequências*, ou uma combinação dessas duas entidades. Isto leva a que um risco seja frequentemente expresso como uma combinação do impacto de uma das possíveis consequências de um evento com a *likelihood* de ocorrência desse evento. Nota para o uso do termo inglês *likelihood* já que, em inglês, *probability* é considerado um termo matemático e não um termo de significado amplo como é *probabilidade* em português ou *likelihood* em inglês; a tradução mais próxima de *likelihood* seria *verosimilhança*.

Outro termo relevante é o de *risk owner* (dono do risco) que é a pessoa ou entidade que tem autoridade ou que é responsável[5] pela gestão de um certo risco. Também existe o termo *controlo*¸ que se refere a uma medida que modifica o risco. [4] [5]

Em [5], define-se também o termo *gestão de risco*. Considera-se que esse conceito corresponde a um conjunto de "atividades coordenadas para dirigir e controlar uma organização no que ao risco diz respeito"[6]. Como tal, a gestão de risco deve possibilitar a maximização dos riscos com efeitos positivos (oportunidades) e a minimização de riscos com efeitos negativos (ameaças).

2.1.1. ISO 31000 – Os Onze Princípios Básicos da Gestão de Risco

A norma ISO 31000 fornece onze princípios básicos que servem de guias para a conceção de uma estrutura de gestão de risco numa organização. Segue-se uma tradução livre dos mesmos (a versão original encontra no Apêndice **A.1. ISO 31000 – Os Onze Princípios Básicos em Inglês**). [4]

1. **A gestão de risco cria e protege valor**: Gestão de risco contribui para a concretização demonstrável de objetivos e para a melhoria de *performance* em, por exemplo, saúde e segurança pública, conformidade legal e reguladora, aceitação pública, proteção ambiental, qualidade do produto, gestão de projetos, eficiência das operações, governança e reputação.

[3] Tradução livre da definição utilizada em [5]: “effect of uncertainty on objectives”.
[4] Tradução livre da definição utilizada em [5]: “the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood”.
[5] *Responsável* é uma tradução lata; em [4] e [5], diz-se que o dono do risco tem a *accountability* (prestação de contas) relativa ao risco.
[6] Tradução livre da definição utilizada em [5]: “coordinated activities to direct and control an organization with regard to risk”.

2. **A gestão de risco é uma componente integral de todos os processos de uma organização**: Gestão de risco é uma atividade que não deve ser separada das principais atividades e processos da organização. A gestão de risco faz parte das responsabilidades da gestão de topo e é parte integral de todos os processos organizacionais, incluindo planeamento estratégico e todos os processos de gestão de projetos.
3. **A gestão de risco faz parte da tomada de decisão:** Gestão de risco auxilia os decisores a tomarem escolhas informadas, a priorizarem ações e a distinguir os efeitos resultantes de várias ações alternativas.
4. **A gestão de risco lida com a incerteza, explicitamente**: A natureza dessa incerteza, e como a mesma pode ser enfrentada.
5. **A gestão de risco é sistemática, estruturada e ocorre no tempo certo**: Uma abordagem à gestão de risco que seja sistemática, estruturada e na altura certa contribui para eficiência e para resultados consistentes, comparáveis e fiáveis.
6. **A gestão de risco baseia-se na melhor informação disponível**: Os *inputs* do processo de gerir riscos são baseados em fontes de informação como históricos, experiência, *feedback* de *stakeholders*, observação, previsões e peritagens. No entanto, decisores devem-se informar sobre, e devem considerar, quaisquer limitações dos dados utilizados ou a possibilidade de divergência entre peritos.
7. **A gestão de risco é personalizada**: Gestão de risco está alinhada com os contextos interno e externo de uma organização e com o perfil de risco.
8. **A gestão de risco tem em conta fatores socioculturais**: Gestão de risco reconhece as capacidades, perceções e intenções de indivíduos que, interna ou externamente, podem facilitar ou dificultar a concretização dos objetivos da organização.
9. **A gestão de risco é transparente e inclusiva**: Envolvimento apropriado de *stakeholders* e, em particular, de decisores de todos os níveis da organização, assegura que a gestão de risco permanece relevante e atualizada. Esse envolvimento também possibilita aos *stakeholders* a expressão dos seus pontos de vista para que os mesmos possam ser apreciados pelos decisores na determinação do critério dos riscos (*risk criteria*).
10. **A gestão de risco é dinâmica, iterativa e responsiva a mudanças**: À medida que ocorrem eventos internos e externos, contexto e conhecimento alteram-se, monitorização e revisão são levados a cabo, novos riscos surgem, alguns mudam, e outros desaparecem. Como tal, a gestão de risco responde continuamente a mudanças.
11. **A gestão de risco facilita a melhoria contínua da organização**: Organizações devem desenvolver e implementar estratégias para melhorar a sua maturidade de gestão de risco assim como todas as restantes vertentes da sua organização.

2.1.2. ISO 31000 – Conceção de uma Estrutura para Gestão de Risco

Os próximos parágrafos destinam-se a analisar como proceder à conceção de uma estrutura para gestão de risco de acordo com as recomendações da norma ISO 31000. Uma estrutura para gestão de risco é definida em [5] como um "conjunto de componentes que fornecem as bases e arranjos organizacionais para a conceção, implementação, monitorização, revisão e melhoria contínua da gestão de risco na organização"[7].

Como exibido na **Figura 5**, para a conceção de uma estrutura, é necessário analisar o compromisso da gestão de topo (*mandate and commitment*) para assegurar a eficiência da gestão de risco. É necessário um compromisso contínuo por parte dos decisores, assim como um planeamento estratégico rigoroso, para que tal compromisso amonte a todos os níveis da organização. [4]

Esse compromisso influencia e é influenciado pela conceção da estrutura para a gestão de risco. De modo a desenhar esse modelo é necessário: (1) um entendimento da organização e do contexto em que está inserida; (2) estabelecimento de uma política de gestão de risco; (3) *accountability* (prestação de contas); (4) integração em processos organizacionais; (5) recursos; (6) estabelecimento de mecanismos para comunicação interna e externa e para relatos.

Segue-se um ciclo **PDCA** (**P**lan – **D**o – **C**heck - **A**ct), para garantir a qualidade da estrutura. A fase de *conceção* corresponde ao planeamento (*plan*) nesse ciclo. O desenvolvimento (*do*) corresponde à implementação da estrutura e dos processos de gestão de risco na organização. A verificação (*check*) corresponde à monitorização e revisão do modelo. Por último, na fase de atuação (*act*), corrigem-se falhas identificadas na fase anterior. Deste modo, garante-se uma melhoria contínua da estrutura. De qualquer modo, organizações devem sentir-se confortáveis em adaptar componentes do sistema descrito para melhor abraçar as suas necessidades.

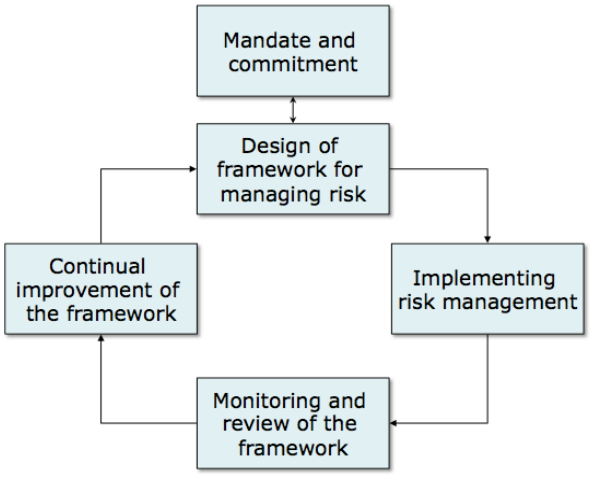

Figura 5 – Estrutura para gestão de risco na norma ISO 31000

[7] Tradução livre da definição utilizada em [5]: "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization".

Assim sendo, uma estrutura de gestão de risco deve incluir processos de gestão de risco assim como os recursos necessários para a sua implementação. Um dos recursos mais utilizados é a ferramenta frequentemente denominada de *registo de riscos*. Idealmente cada *silo* de gestão de risco em uma organização (ex.: corrupção, logística, segurança,…) deveria possuir um registo de riscos próprio; concebido em conformidade com o processo de gestão de risco usado nesse *silo*. [4]

2.1.3. ISO 31000 – Processos de Gestão de Risco

Conforme definido em [5], um *processo de gestão de risco* é a "aplicação sistemática de políticas, procedimentos e práticas de gestão nas atividades de comunicação, consulta, estabelecimento do contexto, e identificar, analisar, avaliar, tratar, monitorizar e rever riscos"[8]. A **Figura 6** exibe um diagrama de um processo de gestão de risco de acordo com a norma ISO 31000. O processo deve ser "uma parte integral da gestão" e "incorporada na cultura e práticas" mesmo estando o mesmo sujeito a customização de modo a que sejam contabilizadas as necessidades específicas da organização. [4]

Comunicação e consulta (*communication and consulting*) são fundamentais a fim de se garantir a definição correta do contexto em que se insere a organização; para esse fim, são levados em conta parâmetros tanto internos como externos. Nesta fase, definem-se também o âmbito (*scope*) e o *risk criteria* para o resto do processo. De qualquer modo, comunicação deve estar também presente ao longo de todas as restantes fases de um processo de gestão de risco.

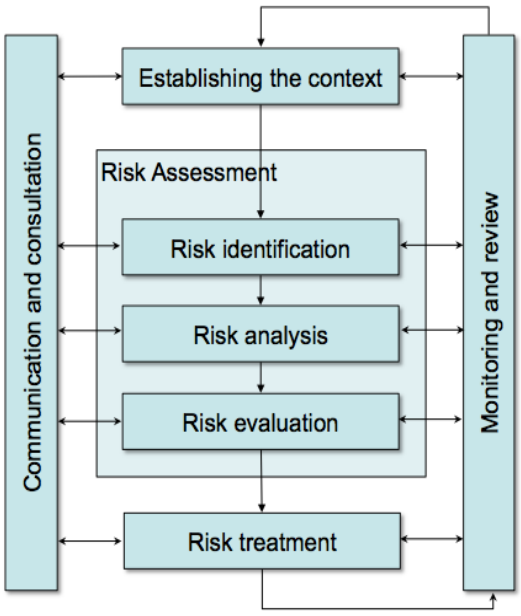

Figura 6 – Processo de gestão de risco na norma ISO 31000

[8] Tradução livre da definição utilizada em [5]: "systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk"

Depois de se ter estabelecido o contexto em que a organização se insere, procede-se a uma apreciação de riscos (*risk assessment*). Nesta fase do processo, espera-se que cada risco seja:

1. Identificado (procurar eventos que possam "criar, aumentar, prevenir, degradar, acelerar ou atrasar a concretização de objetivos"[9]);
2. Analisado (para determinar se o risco precisa de passar por uma fase de tratamento e qual o tipo de tratamento a utilizar);
3. Avaliado (para comparar o nível de risco encontrado na *risk analysis* com o *risk criteria* previamente criada.

Dependendo dos resultados obtidos na apreciação de riscos, a organização deve avançar com o seu processo de gestão de riscos. A fase seguinte é a de tratamento dos riscos (*risk treatment*), na qual se devem selecionar e implementar estratégias para modificação dos riscos que se considerou necessitarem de tratamento (podem ser mitigação de riscos, planos de contingência,…). Conforme estabelecido em [5], o "risco que permanece após o tratamento do mesmo"[10] é denominado de risco residual (*residual risk*). Por último, a fim de garantir a melhoria continua em todas as fases do processo de gestão de risco, é necessário que, em cada uma, se proceda regularmente a operações de monitorização e revisão (*monitoring and review*).

2.2 ISO 31000 – Documentos Complementares

A norma ISO 31000, assim como o ISO Guide 73 e a norma ISO 31010, são frequentemente referidos como sendo a família de normas ISO 31000. Por isso, quando o termo *ISO 31000* é mencionado na literatura, os autores estão frequentemente a referir-se ao conjunto desses três documentos.

As definições apresentadas em *ISO Guide 73: Risk Management - Vocabulary* são geralmente aceites pela comunidade científica e académica como as mais relevantes na gestão de riscos. O vocabulário utilizado na norma ISO 31000 está definido nesse documento, cujo propósito é o de fornecer vocabulário genérico para toda a gestão de risco. Como gestão de risco deve ser específica para cada organização, pode ser necessário complementar o vocabulário no documento ISO Guide 73; no entanto, deve-se dar preferência às definições expostas no mesmo.

A terminologia da gestão de risco está organizada no ISO Guide 73 de acordo com o formato que se segue: (1) termos relacionados a *risco*; (2) termos relacionados a *gestão de risco*; (3) termos relacionados ao *processo de gestão de risco*; (4) termos relacionados a *comunicação e consulta*; (5) termos relacionados ao *contexto*; (6) termo relacionado a *apreciação de risco*; (7) termos relacionados a *identificação de risco*; (8) termos relacionados a *análise de risco*; (9) termos relacionados a

[9] Tradução livre da definição utilizada em [4]: "create, enhance, prevent, degrade, accelerate or delay the achievement of objectives".

[10] Tradução livre da definição utilizada em [5]: "risk remaining after risk treatment".

avaliação de risco; (10) termos relacionados a *tratamento de risco*; (11) termos relacionados a *monitorização e medição*. [5]

Apreciação de risco é definida pelo ISO Guide 73 como sendo o "processo conjunto de identificação de riscos, análise de riscos e avaliação de riscos"[11]. E, de acordo com a norma ISO 31000, a apreciação de riscos é uma componente fundamental de qualquer processo de gestão de risco. Assim se explica a existência de *ISO 31010: Risk Management – Risk Assessment Techniques*; documento esse que tem como finalidade assistir organizações na apreciação de riscos. ISO 31010 inclui uma listagem exaustiva de todas as técnicas ou ferramentas de gestão de risco relevantes para o seu âmbito assim como uma comparação entre essas técnicas; recomenda as fases da apreciação de risco em que certa ferramenta é mais eficaz, e como aplicar as mesmas.

No Apêndice **A.2. Lista de Ferramentas e Técnicas para um Processo de Apreciação de Risco**, é apresentada uma lista das técnicas e ferramentas mais relevantes para a fase de apreciação de risco num processo de gestão de riscos. Na mesma, é identificada a aplicabilidade de cada uma dessas ferramentas em cada momento da apreciação de risco (identificação de risco, análise de risco, e avaliação de risco). Exemplificando, a técnica denominada *fault tree analysis* é fortemente recomendada na análise da probabilidade (*likelihood* é o termo correspondente na norma ISO 31000) de ocorrência do evento associado ao risco; no entanto, não é recomendada a sua aplicação para fins de análise do impacto da consequência associada ao risco. Noutro exemplo, uma *cause-and-effect analysis* é fortemente recomendada para a identificação do risco mas não para a avaliação do mesmo. [6]

2.3 Esforços Institucionais em Gestão de Risco para Corrupção

Corrupção é descrita em [7] como sendo uma "praga que pode ser encontrada em todos os países — grandes ou pequenos, ricos ou pobres — (…) corrupção prejudica os pobres desproporcionadamente devido a desvio de fundos que deveriam ser usados para o desenvolvimento, devido à fragilização da capacidade de um Governo em fornecer serviços básicos, devido ao incentivo à desigualdade e à injustiça, e devido ao desencorajamento de qualquer apoio e/ou investimento externo"[12]. Estas são consideradas as principais razões por detrás da elaboração da *United Nations Convention against Corruption* (**UNCAC**). Nesse documento, apresentam-se os motivos que levaram as Nações Unidas (*United Nations* (**UN**)) a criar essa ferramenta de combate à corrupção. A **UNCAC** é o único instrumento universal juridicamente vinculativo para combate à

[11] Tradução livre da definição utilizada em [5]: "overall process of risk identification, risk analysis and risk evaluation".

[12] Tradução livre da definição utilizada em [7]: "(…) an insidious plague that (…) is found in all countries—big and small, rich and poor— (…) corruption hurts the poor disproportionately by diverting funds intended for development, undermining a Government's ability to provide basic services, feeding inequality and injustice and discouraging foreign aid and investment"

corrupção e, apesar de a sua implementação ser da responsabilidade dos vários governos de Estado, a **UNCAC** é aplicável em todos os setores da sociedade[13].

A **UNCAC** encontra-se dividida em oito capítulos onde são descritas recomendações genéricas a serem seguidas pelos vários Estados: (1) disposições gerais, (2) medidas preventivas, (3) criminalização e cumprimento da lei, (4) cooperação internacional, (5) recuperação de ativos (*asset recovery*), (6) assistência técnica e troca de informação, (7) mecanismos de implementação; (8) disposições finais. Esses oito capítulos amontam a um total de setenta e um artigos.

De modo a suportar a Convenção, foi lançada em 2011 uma biblioteca jurídica para a **UNCAC** como uma base de dados co-fundada pela iniciativa *Stolen Asset Recovery* (**StAR**), que é um programa conjunto do *World Bank Group* e do Escritório das Nações Unidas sobre Drogas e Crime. Nessa biblioteca, é possível aceder à legislação de combate a corrupção de 178 Estados.

Em dezembro de 2009, a União Europeia apresentou o *Programa de Estocolmo*. A sua finalidade foi a de auxiliar estados-membro da União Europeia a lidar com questões relacionadas com justiça, entre as quais se incluíam problemas de corrupção, através da aplicação de recomendações válidas de 2010 a 2014.

2.4 Análise Comparativa da Corrupção em Indústrias Distintas

De acordo com [8], existem quatro fatores comportamentais de relevância que se encontram correlacionados com atos de corrupção: (1) desejo de alcançar uma meta pessoal ou profissional; (2) normas subjetivas; (3) *Perceived Behavioral Control* (a facilidade de um indivíduo em realizar um dado comportamento); (4) atitude. Mais, também se conclui em [8] que a intenção de concretizar uma meta pessoal ou profissional assim como a viabilidade da sua concretização não estão correlacionadas com o ato de corrupção a si associado. Tal implica que *desejo* (dependente de emoções de um indivíduo consoante uma dada situação) pode ser um catalisador mais efetivo para a ocorrência de atos relacionados com corrupção; enquanto que *intenção* (estado mental resultante de deliberação) não tanto.

Todavia, o estudo conduzido em [8] concentrou-se na indústria da construção e obras. Assim sendo, importa verificar até que ponto as conclusões retiradas desse mesmo estudo se aplicam noutras indústrias. A **Figura 7** exibe alguns dos principais fatores de risco de corrupção para quatro indústrias distintas: a de construção e obras, de petróleo e gás, das ciências da vida, e de extração de minerais.

Um fator de risco que parece ser comum às várias indústrias é o uso de terceiros (seja em *joint-ventures* ou seja através do uso de consultores ou agentes). Além disso, processos com vários pontos de contato com oficiais governamentais são um problema comum à maior parte das indústrias. Estima-se que esses funcionários exijam subornos mais frequentemente devido a receberem remunerações inferiores a trabalhadores com funções semelhantes fora da função pública.

[13] Conforme explícito em: http://www.track.unodc.org/Pages/home.aspx.

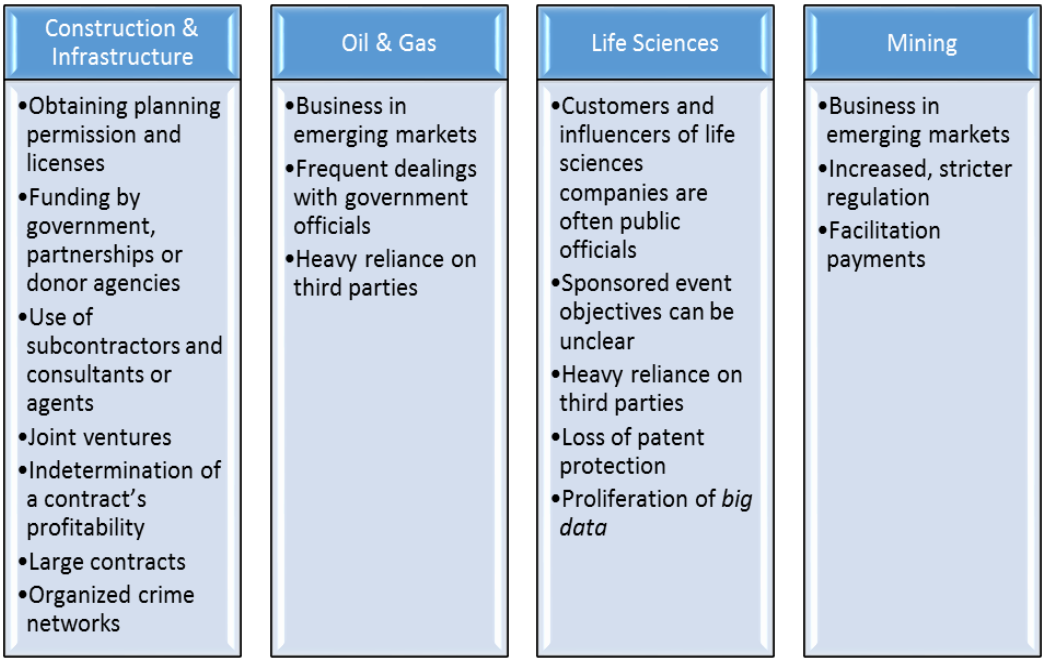

Figura 7 – Principais fatores de risco de corrupção em indústrias distintas (em inglês)

Por último, a expansão de algumas indústrias para mercados emergentes é outro fator de risco significativo, já que se calcula que essas regiões tenham um alto risco de corrupção. De qualquer modo, existem alguns fatores de risco específicos para algumas das indústrias analisadas. [9] [10] [11] [12]

Na indústria da construção e obras, a obtenção de licenças é um processo arrastado no tempo, e que fica assim mais facilmente sujeito à ocorrência de abusos. Além disso, já que negociações relacionadas com a adição de especificações técnicas e com custos excessivos são críticas para determinar a rentabilidade de um contrato, consultores ou clientes têm uma oportunidade de obter benefícios indevidos por via de corrupção. Mais, redes criminosas organizadas exploram frequentemente setores onde os trabalhadores têm uma elevada carga de trabalho como o da construção e obras. [9]

Na indústria das ciências da vida, objetivos dos *sponsors* são frequentemente pouco claros, isto é, não é possível determinar se um determinado evento está ou não relacionado com puro intercâmbio científico ou com táticas promocionais por parte do *sponsor*. Perda de proteção das patentes é também uma preocupação já que aumenta a pressão para se manter uma certa quota de mercado; o que por sua vez pode levar empregados a praticarem atividades progressivamente agressivas. Por último, o aumento da concorrência e a publicação de legislação cada vez mais rigorosa levam a que a gestão de um programa de combate à corrupção seja progressivamente mais complexa devido ao elevado número de dados a analisar (*big data*). [11]

O aumento da importância da *big data* é também motivo de preocupação na indústria de extração de minerais; assim como o fenómeno de "pagamentos facilitadores" (*facilitation payments*),

pagamentos oficiosos a funcionários públicos para assegurar ou acelerar a *performance* de uma rotina ou ação necessária. [12]

2.5 ISO 37001 – Norma para Gestão de Sistemas de Combate ao Suborno

Em 2013, o *World Bank* constatou que a ***OECD*** *Anti-Bribery Convention* (ratificada pelo Estado Português) já tinha resultado na sanção de trezentos e trinta e três indivíduos e de cento e onze organizações devido a crimes de suborno, para além de trezentas e noventa investigações a decorrerem em vinte e quatro territórios distintos. [13]

São dados como esses que levam a **ISO** a considerar suborno como um dos maiores desafios para Governos e empresas em todo o mundo. Assim sendo, essa instituição encontra-se a desenvolver a norma ISO 37001, uma proposta para a gestão de sistemas de combate ao suborno, cujo objetivo será o de auxiliar a implementar ou melhorar esses sistemas nas organizações. A norma ISO 37001 especificará medidas que a organização deve seguir de modo a prevenir, detetar e lidar com suborno, e recomendações para a implementação dessas mesmas medidas.

A norma ISO 37001 poderá ser adaptada à dimensão e natureza da organização assim como ao risco de suborno que enfrenta. Uma organização pode beneficiar desta norma via: (1) assistência na implementação/melhoria de um sistema de combate ao suborno; (2) garantir fiabilidade à gestão de topo, investidores, e outros parceiros de negócios da organização; (3) em caso de ocorrência de investigações criminais, fornecimento de prova a tribunais e procuradores de como a organização tinha tomado medidas para prevenir a ocorrência de subornos.

No dia 3 de novembro de 2015, um *Draft International Standard* (**DIS**) para a norma já tinha sido registado. Em 14 de abril de 2016, a **ISO** anunciou que o **DIS** tinha sido aprovado com 91% dos votos dos membros da organização envolvidos na criação da norma. O *draft* da norma já pode ser adquirido, no entanto, a versão final da mesma só deverá ser publicada em finais de 2016. [14]

No entanto, esta norma foca-se exclusivamente em suborno, não em extorsão ou conflitos de interesses, que também pertencem ao domínio da corrupção (como se pode ver na **Figura 1**). Mais, esta norma é alvo de algumas críticas, como o facto de ter um foco muito grande na apreciação de riscos, o que o torna muito semelhante à norma ISO 31000[14].

2.6 Conclusões do Capítulo

No presente capítulo, foi conduzida uma revisão de literatura sobre gestão de risco. Iniciou-se a mesma com definições consideradas relevantes segundo o ISO Guide 73 para o entendimento da gestão de risco.

[14] Opinião retirada de: http://www.natlawreview.com/article/antibribery-international-organization-standardization-37001-new-measuring-stick.

Seguiu-se para o estudo da norma ISO 31000, que é adotada por cada vez mais países (incluindo Portugal) como a norma nacional oficial de gestão de risco. Foram exibidos os onze princípios básicos da gestão de risco segundo essa norma, e a ligação dos mesmos com a conceção de uma estrutura e de processos de gestão de risco numa organização. Estudaram-se também os dois documentos que complementam a norma ISO 31000, ou seja, a norma ISO 31010 e o já mencionado ISO Guide 73.

Foram listados alguns dos mais relevantes esforços institucionais para a gestão de riscos no âmbito da corrupção e infrações conexas como, por exemplo, a **UNCAC**; concluiu-se também que é escassa a literatura de carácter académico sobre aplicação de princípios de gestão de risco na corrupção, comparativamente à literatura de carácter institucional. De seguida, compararam-se fatores comuns e específicos para várias indústrias que pudessem ser catalisadores de corrupção e, por último, foi revisto o estado da norma de combate ao suborno ISO 37001.

3. Análise e Solução do Problema

O presente capítulo é composto por três partes principais. Primeiro, procurar-se-á aplicar o conhecimento adquirido na revisão da literatura a um breve caso de estudo correspondente ao plano de gestão de riscos do *Metro Lisboa*. Pretendem-se inferir conclusões sobre métodos seguidos pelas várias organizações, ilustrando isso com o exemplo do *Metro Lisboa.* Também se pretende averiguar falhas que sejam comuns a uma grande parte dos relatórios usando, mais uma vez, o exemplo do *Metro Lisboa* para ilustração.

De seguida, será conduzida uma análise à ferramenta *registo de riscos*, pretendendo-se concluir que o uso dessa ferramenta de acordo com as boas-normas da gestão de risco poderá ser uma solução efetiva para o problema deste trabalho.

Para concluir, ir-se-á procurar validar essa solução mediante o uso de um processo que estruturará os dados reais da **INCM**, do **IST** e do **LNEC** consoante o modelo de informação definido.

3.1 Análise de Caso – Metro Lisboa

De acordo com [2], apenas um estimado de 41.2% das mesmas seguiu um método formal de gestão de risco. 9.3% seguiram a FERMA, 9.2% COSO, 10.1% seguiram ambas e 12.6% seguiram a norma ISO 31000 ou outro método de gestão de risco distinto. Esta informação permite retirar algumas conclusões. Em primeiro lugar, tal possibilita corroborar a existência de uma heterogeneidade significativa nos planos desenhados. Importa destacar também que, em vários planos, não foi percetível o uso de qualquer estrutura de gestão de risco.

O caso de estudo que se segue consiste no plano de gestão de riscos elaborado pelo *Metro Lisboa*. Utiliza-se este caso por se considerar que o plano elaborado pelo *Metro Lisboa* é um dos melhor elaborados e por permitir comprovar como a aplicação de um método bem definido por uma organização leva a uma maior qualidade na gestão de risco. Mas, por outro lado, pretende-se mostrar também que, mesmo assim, haveria margem para melhorias nesse plano. É verdade que a norma ISO 31000 define um conjunto de conceitos e princípios, mas não prescreve nenhum dos mesmos; no entanto, com a informação definida, não é possível retirar certas conclusões que contribuiriam ainda mais para a prevenção da corrupção nesta organização.

Iniciando a análise deste plano de gestão de riscos, é visível que se seguiu um método assente no **ACFE** *Fraud Risk Manual*, classificando-se riscos de fraude de acordo com as seguintes quatro categorias:

1. Corrupção;
2. Conflitos de interesse;
3. Apropriação indevida de ativos;
4. Manipulação de informação.

1. Corrupção
1.A) Corrupção ativa / suborno, exercida sobre:
1.A.1) Exterior (empresas e indivíduos)
1.A.2) Colaboradores (incluindo através de compensações internas não justificadas)
1.B) Corrupção passiva
1.B.1) Concursos / elaboração de contratos
1.B.2) Adjudicações diretas
1.B.3) Processos judiciais / contenciosos / falsos testemunhos
1.B.4) Atribuição de patrocínios / subsídios / donativos
1.B.5) Aplicação de coimas / multas
1.B.6) Subfaturação
1.B.7) Sobrefaturação
1.B.7.a) Materiais
1.B.7.b) Prestação de serviços
1.B.7.c) Trabalho a mais / menos
1.B.7.d) Horas
1.B.8) Recebimentos ilegais através de dinheiro / presentes / viagens / entretenimento / outros
1.B.9) Extorsão económica

Figura 8 – Classificação usada pelo *Metro Lisboa* para gestão de risco (Fonte: [15])

Por sua vez, essas categorias mencionadas pela **ACFE** são divididas em subcategorias apropriadas que sejam adequadas à realidade em que se insere o *Metro Lisboa*. A **Figura 8** é a classificação usada pela organização conforme surge em [15]. Por exemplo, a categoria principal *corrupção* é dividida em duas subcategorias: *corrupção ativa* e *corrupção passiva*. Este ajuste no modelo assegura a sua conformidade com a legislação Portuguesa já que, em Portugal, corrupção é considerada ou ativa ou passiva. *Corrupção ativa* refere-se a um indivíduo que corrompe, enquanto que *corrupção passiva* refere-se a um indivíduo que se deixa corromper[15]. [15]

Encontramo-nos então perante um caso em que é percetível o uso de um método formal de gestão de risco, neste caso partindo do manual da **ACFE**. É de notar que, apesar de o *Metro Lisboa* não mencionar que segue a norma ISO 31000, a organização ajusta o método seguido de acordo com o contexto em que está inserida; ou seja, é uma adaptação de recomendações genéricas a uma organização específica, o que é encorajado pela norma ISO 31000.

Além disso, a utilização de classificações semelhantes à utilizada pelo *Metro Lisboa* é frequentemente útil na medida em que simplifica a implementação de gestão de risco numa organização.

Todavia, se olharmos à **Figura 9**, pode-se constatar que, ao não seguir a norma ISO 31000, o registo de riscos do *Metro Lisboa* acaba por exibir algumas lacunas. Em primeiro lugar, segundo a norma ISO 31000, um risco é composto pela relação entre um evento e uma consequência. Ora, na ilustração apresentada, pode-se comprovar que não há qualquer menção de evento ou consequência. Mais, nesta ilustração em concreto, confere-se que os casos mencionados pelo *Metro Lisboa* não são *riscos* mas sim *consequências*.

[15] Retirado de: http://www.dgpj.mj.pt/sections/informacao-e-eventos/prevenir-e-combater-a/anexos/definicao-de-corrupcao/.

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas no ML			
Identificação dos Riscos	**CR**	**Função ou Atividade**	**Medidas de Prevenção**
1 – Corrupção			
A) Corrupção ativa/suborno, exercida sobre:			
1) Exterior (empresas e indivíduos)	1B	Relacionamento com entidades externas	**(a)** Conforme previsto no Código de Ética e de Conduta os colaboradores do ML têm o dever de observar e de fazer observar os princípios e compromissos do "*Global Compact*" e de denunciar qualquer situação que viole esses princípios. **(a)** As auditorias de certificação são sempre acompanhadas por mais de um elemento do ML e o IPAC pode vir verificar in loco sem aviso a atuação da entidade certificadora. **(a)** Periodicamente existe mudança de empresa para a auditoria às contas anuais. **(a)** Valores comunicados de vendas de títulos são confrontados com os valores registados no sistema de venda. As diferenças são objeto de análise sistemática. **(a)** A generalidade da faturação dos fornecedores é confrontada com os pedidos de compra (contratos e notas de encomenda). **(b)** Auditoria ao sistema de recolha de receitas tarifárias.
2) Colaboradores (incluindo remunerações e compensações não justificadas)	1A	Gestão de recursos humanos	**(a)** As remunerações / compensações estão previstas nos Acordos de Empresa e são processadas pela RHC com base na informação que resulta do registo e controlo de assiduidade. **(a)** Os colaboradores do ML devem promover a salvaguarda dos princípios estruturantes e valores centrais da empresa (Código de Ética e de Conduta). **(b)** Auditoria ao processamento de remunerações e complementos de reforma.

CR - Classificação do Risco: Combinação de Probabilidade (1 = Baixa; 2 = Média e 3 = Alta) e Impacto (A = Baixo; B = Médio e C = Alto).

Medida preventiva do Risco: (a) Implementada; (b) A implementar.

Figura 9 – Registo de riscos do *Metro Lisboa* para gestão de risco (Fonte: [15])

Esta aparente confusão entre os conceitos de *risco*, *evento* e *consequência* torna-se mais evidente quando se verifica que o *Metro Lisboa* classifica cada "risco" por *probabilidade* e *impacto*, conceitos que correspondem a *evento* e *consequência* respetivamente. Neste contexto, faria mais sentido classificar cada caso por *nível de risco*, no entanto, esse atributo dependeria da probabilidade do evento e do impacto da consequência; e como já se constatou, o *Metro Lisboa* não está a considerar o *risco* como a relação entre um *evento* e uma *consequência*.

Por último, não é especificado qualquer *dono de risco* em nenhum caso, apenas medidas de prevenção.

Assim se conclui que este registo de riscos é útil e encontra-se bem-organizado de acordo com o contexto da empresa, o que auxilia a gestão de risco na mesma. No entanto, ao não seguir a norma ISO 31000, verifica-se também que este plano tem lacunas que diminuem a qualidade da gestão de risco na organização. Importa salientar que a maior parte das lacunas anteriormente mencionadas são comuns a quase todos os *Planos de Gestão de Riscos de Corrupção e Infrações Conexas*.

3.2 Modelos de Registos de Riscos

Praticamente todas as organizações estudadas utilizaram uma versão própria de um registo de riscos. De acordo com [5], um registo de riscos é um "arquivo de informação sobre riscos

identificados”[16]. Isto é, esta ferramenta funciona como um arquivo de todos os riscos identificados por uma organização e fornece informação sobre vários aspetos desses riscos como, por exemplo, dono do risco ou medidas para controlo do mesmo. Apesar de os “registos de riscos” não serem mencionados na norma ISO 31000, esse documento não deixa de realçar a importância da documentação de riscos numa organização. [4]

Registos de riscos podem levar indivíduos a terem a “ilusão de controlo”, isto é, terem a sensação de controlo sobre acontecimentos que estes não influenciam. No entanto, se usados com bom senso, os registos de riscos são uma ferramenta útil na gestão de risco de qualquer empresa. [16]

Assim sendo, decide-se testar a possibilidade de utilizar a ferramenta *registo de riscos* para solucionar o problema exposto neste trabalho. O modelo do registo de riscos depende do contexto do problema, pelo que o estabelecimento do contexto no processo de gestão de risco respetivo mostra-se então essencial à customização desta ferramenta numa organização. Em suma, um registo de riscos pode conter tantos itens quanto uma organização desejar; no entanto, um registo com muitos itens pode ser demasiado complexo e não acrescentar valor à gestão de risco.

A conceção de um registo de riscos pode tornar-se então num desafio para as organizações; o objetivo deverá passar por ter um registo com o máximo de itens possíveis até que o valor acrescentado pela adição de mais um item não compense o aumento de complexidade a que se deve o mesmo.

Analisando a norma ISO 31000 e os seus principais conceitos, propõe-se um modelo que seja conceptualmente semelhante ao apresentado na **Figura 10**. Nesse modelo de domínio, um dado *risco* encontra-se associado a um *evento* e a uma *consequência*. Existe uma *likelihood* de ocorrência do *evento* e, dependendo da *consequência* em questão, o seu *impacto* será distinto. Um risco também deverá ter a si associado um *controlo*. Por último, pode-se considerar o conceito de *dono de risco* como sendo uma entidade em si mesma apesar de, no modelo apresentado na **Figura 10**, surgir como um atributo da entidade *risco*.

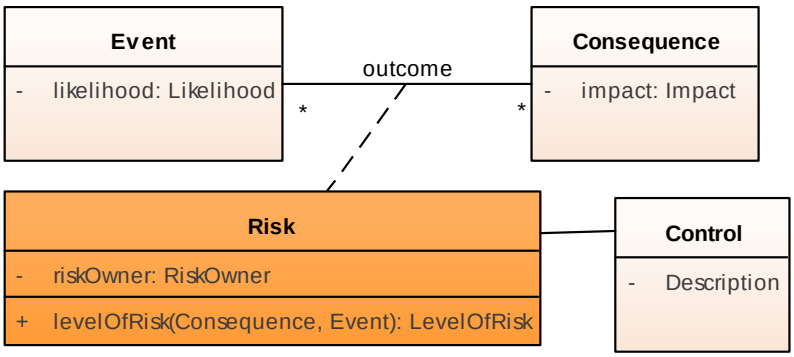

Figura 10 – Modelo de registo de riscos proposto

[16] Tradução livre da definição utilizada em [5]: “record of information about identified risks”.

Este modelo de registo de riscos é simples na medida em que apenas contém os que se consideram ser os principais conceitos da gestão de riscos segundo a norma ISO 31000. Aliás, voltando ao exemplo da **Figura 9**, pode-se constatar que esse mesmo registo de risco segue uma estrutura semelhante e, embora existam algumas lacunas de informação nesse registo (conforme mencionado na subseção **3.1**), este é um registo útil para a respetiva organização e um dos melhores registos entre as várias organizações Portuguesas. Assim sendo, tendo em conta o contexto deste problema, o uso de um modelo mais complexo não se justifica.

Todavia, na **Figura 11** e na **Figura 12**, apresentam-se modelos alternativos para um registo de riscos. Ambos são significativamente mais complexos, tendo integrado mais conceitos mencionados na norma de gestão de risco ISO 31000.

No modelo da **Figura 11**, um dado *risco* estaria ligado ao *evento* com o qual está associado e à respetiva *consequência*. Existe uma *likelihood* de ocorrência do *evento* e uma *fonte de risco* que despoleta o *evento.* Mais, dependendo da *consequência* em questão, o seu *impacto* será distinto já que cada *consequência* afetará de modo distinto um determinado *objetivo*; no processo de gestão de risco, o efeito de uma consequência em objetivos faz parte do estabelecimento do contexto. Por último, três fatores irão determinar o *controlo* do *risco*: (1) *eliminação da fonte* (nesse caso, o *risco residual* é nulo); (2) *redução da likelihood*; (3) *redução do impacto*.

O uso desse modelo pode parecer tentador; mas, como foi anteriormente mencionado, ter um número excessivo de atributos e entidades num determinado modelo de domínio pode levar a um processo de gestão de risco demasiado complexo. Conclui-se assim que a estrutura que é apresentada na **Figura 11** pode ser desnecessariamente complexa para o contexto do problema em que se insere.

Mesmo a estrutura apresentada na **Figura 12**, na qual apenas se retiram os conceitos de *fonte de risco* e *eliminação da fonte* por comparação ao modelo da **Figura 11**, parece ser demasiado complexa pelos motivos já enunciados.

Assim sendo, para o contexto do problema deste trabalho, sugere-se um modelo para o registo de riscos semelhante ao exposto na **Figura 10**. Um registo de riscos que siga esse modelo é simples o suficiente para a maioria das organizações, mas não deixa de ter os conceitos principais de gestão de risco de acordo com a norma ISO 31000.

Os modelos apresentados na **Figura 10**, **Figura 11** e **Figura 12** são um trabalho em progresso do grupo de pesquisa IDSS no INESC-ID; grupo esse que ajudou à conceção deste trabalho.

Com a exibição destes vários modelos distintos, pretende-se concluir que, embora se proponha um registo de riscos que siga uma estrutura idêntica à exibida no modelo da **Figura 10**, é possível ter registos de riscos conceptualmente diferentes mas que não deixem de seguir as recomendações da norma ISO 31000.

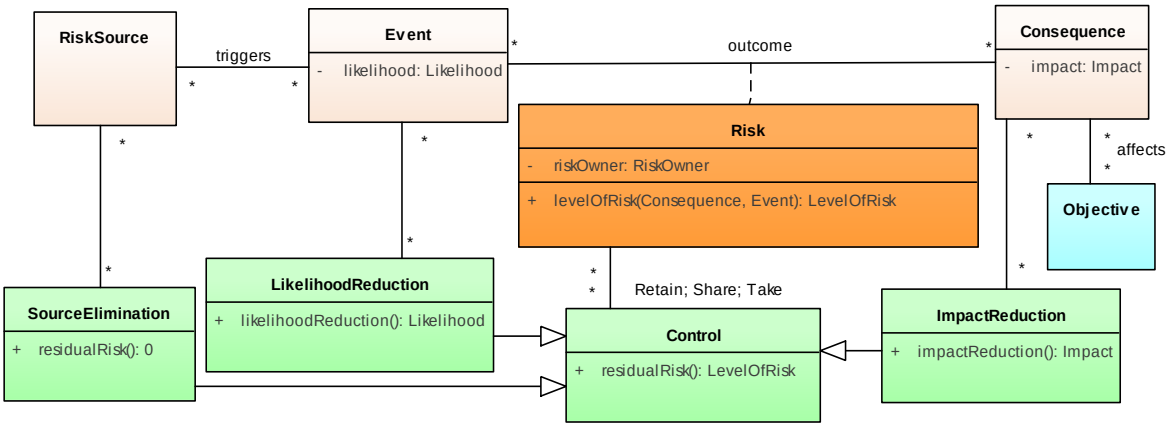

Figura 11 – Modelo alternativo com múltiplos conceitos da norma ISO 31000

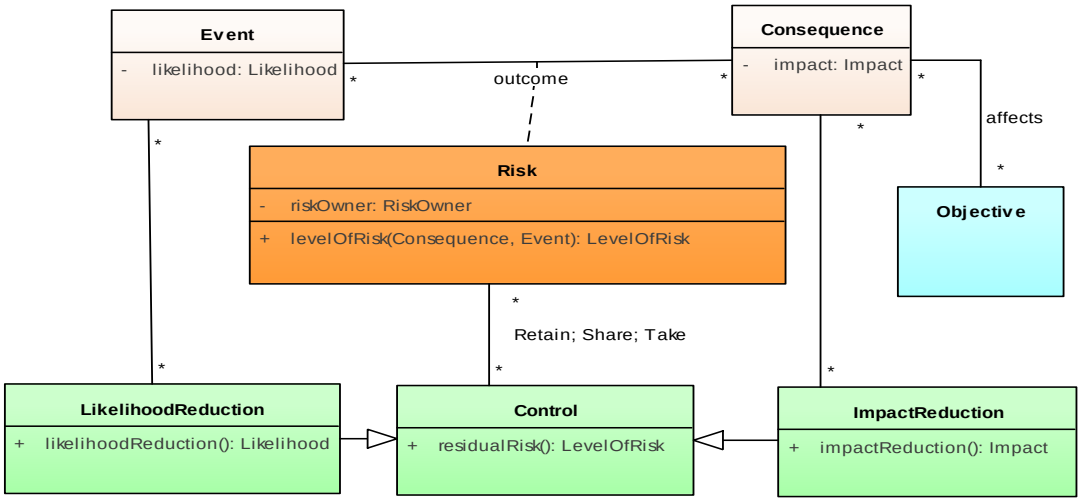

Figura 12 – Versão simplificada do modelo apresentado na Figura 11

3.3 Aplicação e Validação da Solução

A solução deste problema deriva da necessidade de gerir a informação numa estrutura de informação mais adequada e num ambiente que dê flexibilidade. Daí resulta a necessidade de um modelo de registo de riscos de referência válido. Após aplicação do processo a seguir exposto em dados reais de empresas de temáticas variadas, concluiu-se que a solução do problema é, de facto, válida. As empresas estudadas foram a **INCM** (área de produção de bens/serviços para o Estado), o **IST** (área de educação/investigação) e o **LNEC** (área de I&D para engenharia civil).

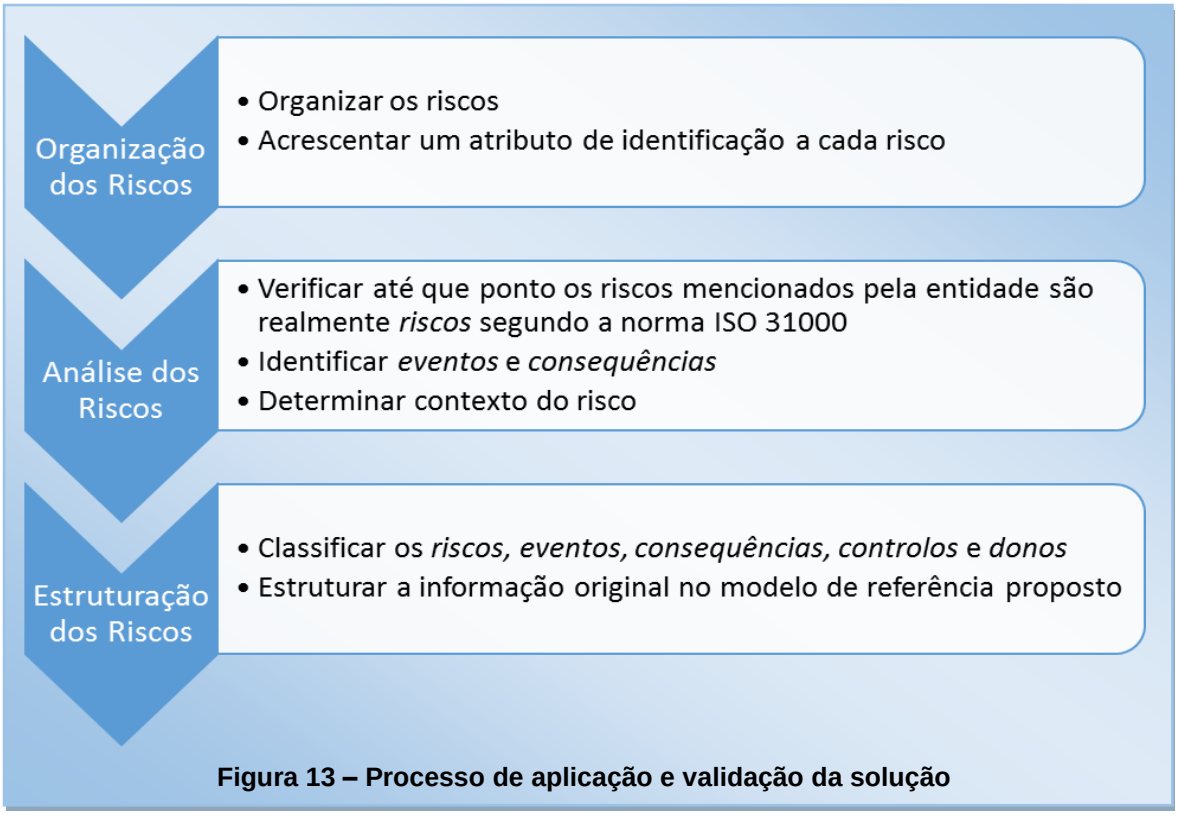

Figura 13 – Processo de aplicação e validação da solução

Como se pode verificar na **Figura 13**, o processo utilizado para gerir essa informação, isto é, o processo de estruturação dos dados reais dessas organizações na estrutura de referência proposta, segue três passos, sendo que em cada um dos mesmos se procura acrescentar valor ao produto final.

O processo que será apresentado e validado já se encontra em utilização por parte da **INCM**; espera-se que a próxima versão do plano de gestão de riscos da **INCM** já contenha as recomendações deste trabalho. Para demonstrar então este processo, serão exibidos exemplos da aplicação do mesmo em dados do plano atual da **INCM**.

3.3.1. Organização dos Riscos

Em primeiro lugar, procede-se à exposição e identificação dos riscos conforme organizados pela organização em causa. É acrescentado um atributo de identificação a cada risco com a finalidade de facilitar a sua rastreabilidade no resto do processo.

Segue-se um exemplo de como a informação fornecida pela **INCM** é transferida para um simples registo em *excel*. Na **Figura 14**, pode-se ver alguns riscos mencionados pela **INCM** conforme expostos no respetivo plano de gestão de risco.

Já na **Figura 15**, é exibida a transcrição desses casos para uma folha de *excel*. O objetivo deste primeiro passo é o de atribuir uma identificação única para cada risco; daí ser-se acrescentado

o atributo **Risco_ID** no primeiro registo. Esta identificação tornará mais eficiente a organização da informação no resto do processo.

Compras

Atividade	Risco	Controlo	Notação	Responsável controlo
Geral.	Favorecimento de terceiros.	Regulamento de Aquisições. C. C. P. — Código dos Contratos Públicos.	Moderado	Todas as áreas DCP
	Quebra de sigilo profissional, revelando informações com intenção de obter benefícios.	Regulamento de Aquisições. Plano de Atividades e Orçamento (PAO).	Fraco	Todas as áreas DCP

Figura 14 – Riscos considerados pela INCM no seu plano de gestão de riscos

	A	B	C	D	E	F	G
1	Risco_ID	Risco_Nome	Nível de Risco	Unidade de Negócio	Atividade	Controlos	Responsável_Controlo
2	RR1	Favorecimento de terceiros	Moderado	Compras	Geral	Regulamento de Aquisições.	Todas as áreas DCP
3	RR2	Quebra de sigilo profissional, revelando informações com intenção de obter benefícios	Fraco	Compras	Geral	Regulamento de Aquisições. Plano de Atividades e Orçamento (PAO).	Todas as áreas DCP

Figura 15 – Transcrição dos casos da Figura 14 para *excel*

É visível que este primeiro passo é relativamente simples; pretende-se apenas organizar a informação já existente numa plataforma própria para o efeito (o *excel* por exemplo), e atribuir uma identificação a cada risco de modo a que, quando se mencione certo código, saiba-se imediatamente de que risco se trata e qual a informação que este comporta. Ao organizar e catalogar a informação neste primeiro passo, os passos que se seguem tornam-se mais fluidos.

3.3.2. Análise dos Riscos

Em segundo lugar, procede-se à análise desses riscos para determinar como se irão estruturá-los. O ponto principal da análise passa por determinar se se está realmente na presença de um risco conforme definido na norma ISO 31000 ou de um evento ou consequência. Se for realmente um risco, procura-se determinar se é apenas um risco (ou seja, a combinação de um evento com uma consequência) ou múltiplos riscos (por exemplo, um evento com duas consequências distintas). Por último, procura-se determinar se o risco pertence ao contexto da corrupção e infrações conexas e, na ausência de informação mais explícita, registam-se as interpretações que foram feitas de cada risco, para que seja percetível o raciocínio por detrás da análise.

Na **Figura 16**, pode-se ver como esta análise foi feita para os riscos expostos na **Figura 15**. Para o "risco" RR1, verificou-se que, na realidade, estava-se na presença de uma consequência, já que não foi possível identificar um evento para a mesma. Já para RR2, foi possível identificar um evento *revelação de informações* e duas consequências: (1) quebra de sigilo profissional; (2) intenção de obter benefícios. Assim sendo, conclui-se que é possível estruturar dois riscos no caso RR2, já

que um risco é composto por apenas um evento e uma consequência. Retira-se então de RR2 os riscos: (1) quebra de sigilo profissional devido a revelação de informações; (2) intenção de obter benefícios via revelação de informações.

Conclui-se também que tanto RR1 como RR2 são relevantes para o âmbito, isto é, pertencem ao contexto da corrupção e infrações conexas. No campo de análise/interpretação, são fornecidos comentários sobre o risco de modo a que a estruturação dos mesmos no próximo passo seja a mais informada possível. Mais, tendo em conta se foi ou não possível identificar evento e/ou consequência, e se um dado risco pertence ou não ao domínio do problema, é atribuída uma de quatro recomendações possíveis a cada caso. Tal será exemplificado na **Figura 17**.

No que diz respeito à identificação de eventos e de consequências, em alguns casos, é possível deduzi-los/as apesar de não serem explicitamente mencionados. Por exemplo, em RR54, deduziram-se as consequências "favorecimento de terceiros" e "concussão" apesar de as mesmas não estarem explícitas na descrição do risco. Em casos menos óbvios, será importante explicar o raciocínio por detrás da dedução de um evento/consequência no campo de "Análise/Interpretação". Depois, em outros casos, não é claro se o risco referido se enquadra ou não no contexto do problema. Em situações dessas, o campo respetivo é assinalado com "??" como também se pode verificar na **Figura 17** (casos RR55 e RR56).

Em relação ao último campo, onde é assinalada a ação que se recomenda tomar relativamente a um dado risco, temos na **Figura 17** exemplos das quatro recomendações possíveis. Essas recomendações são:

1. Manter/Estruturar;
2. Identificar Consequência;
3. Rever;
4. Não constitui um risco.

	A	B	H	I	J	K	L
1	Risco_ID	Risco_Nome	Possível evento?	Possível consequência?	Relevante para o contexto?	Análise/Interpretação	Acção Recomendada
2	RR1	Favorecimento de terceiros	Não	Sim	Sim	A existência de favorecimento de terceiros é já por si uma...	Não constitui um risco
3	RR2	Quebra de sigilo profissional,...	Sim	Sim	Sim		Manter/Estruturar

Figura 16 – Análise dos riscos considerados pela INCM na Figura 14 e expostos na Figura 15

55	RR54	Possibilidade da ocorrência de conflitos de...	Sim	Deduzido	Sim	Deduz-se que pode dar origem a vários riscos de corrupção nomeadamente...	Manter/Estruturar
56	RR55	Incompatibilidades na acumulação de funções	Não	Sim	??	A existência de incompatibilidades na acumulação de funções é já...	Não constitui um risco
57	RR56	Acumulação de funções sem prévia autorização	Sim	Não	??	Identificando o risco como uma possivel causa de corrupção não foi possivel...	Rever
58	RR57	Adulteração das informações relativas ao...	Sim	Não	Sim		Identificar Consequência

Figura 17 – Exemplo das várias ações recomendadas para estruturação de riscos

No caso RR54, verificou-se que este contém, pelo menos, um risco na verdadeira definição da palavra; isto é, foi possível identificar/deduzir pelo menos um evento associado a uma consequência. Como este caso se enquadra no domínio da corrupção e infrações conexas, é recomendado que o mesmo seja estruturado no risco ou riscos correspondentes.

Avançando para o caso RR57, verificou-se que este também se enquadra no contexto do problema. No entanto, apesar de ter sido possível identificar um evento, não se conseguiu identificar nenhuma consequência dessa ação. Nestes casos, assume-se como prioridade verificar junto da organização se este evento pode ter alguma consequência que não se tenha conseguido identificar/deduzir. Caso se consiga eventualmente obter informação para determinar alguma consequência resultante da ação exposta, este risco poderá também ser estruturado de acordo com as boas-normas.

Por último, há que analisar os dois restantes casos. No caso RR56, considera-se não haver informação suficiente para classificá-lo como um risco de corrupção e infrações conexas. Uma vez que aparentemente este caso não pertence num plano de gestão de riscos de corrupção e infrações conexas, é recomendada a revisão do mesmo. Já em RR55, o que se considera merecer maior atenção é a não identificação de qualquer evento. Como já foi mencionado, um risco tem que ter um evento e uma consequência. Nos casos em que se tem um evento mas não se conseguiu determinar uma consequência, assumiu-se que existe uma consequência desconhecida por falta de informação (podendo ou não pertencer ao domínio do problema). Em RR55, acontece o oposto, isto é, o "risco" mencionado é a consequência em si mesma, com incerteza nula. Assim sendo, não se conseguindo apurar causas para a consequência mencionada, considera-se que RR55 não constitui um risco.

É, no entanto, de salientar que o uso destas recomendações é sujeito a interpretação. Exemplificando, RR56 e RR57 também não constituem riscos dado que não existe evento e consequência. No entanto, em RR56 considerou-se mais relevante a revisão do caso uma vez que, mesmo que se identificasse uma consequência, não há informação que nos permita enquadrar RR56 no contexto do problema. É certo que em RR55, também não se consegue determinar o contexto em que se insere um possível risco. Mas, se em RR56, considerou-se que seria possível determinar uma consequência com mais alguma informação; em RR55, considerou-se que dificilmente se conseguiria discernir em evento associado à consequência exposta, pelo que nunca teríamos um risco.

3.3.3. Estruturação dos Riscos

No terceiro passo deste processo de gestão de informação, tendo como guia os resultados da análise conduzida no passo anterior, os riscos são estruturados num registo de riscos com um modelo conceptualmente semelhante ao da **Figura 10**. Sempre que possível, procurar-se-á também acrescentar *flags* a cada risco, evento, consequência ou controlo para uma tipificação mais acessível (especialmente se se utilizar uma plataforma de gestão de risco como a *HoliRisk*).

	A	B	C	D	G	H	N	O	T	U	V
1	Risco				Evento		Consequência		Controlos & Donos		
2	Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Evento_ID	Evento_Nome	Consequência_ID	Consequência_Nome	Controlo_ID	Dono_ID	*Notas do Risco*
3	R1		Moderado	RR1	EV1		CQ1	Favorecimento de terceiros	CONT1; CONT2	DONO1; DONO21	
4	R2	Quebra de sigilo profissional devido a...	Fraco	RR2	EV2	Revelação de informações	CQ2	Quebra de sigilo profissional	CONT1; CONT3	DONO1; DONO21	
5	R3	Revelação de informações para	Fraco	RR2	EV2	Revelação de informações	CQ3	Favorecimento próprio	CONT1; CONT3	DONO1; DONO21	

Figura 18 – Estruturação dos riscos expostos na Figura 15

Na **Figura 18**, pode-se ver como os riscos expostos pela **INCM** estão estruturados de acordo com o processo aqui mencionado. Com a análise efetuada na **Figura 17**, determinou-se que RR1 não é realmente um risco pois o favorecimento de terceiros é a consequência em si mesma, com incerteza nula. Assim sendo, o favorecimento de terceiros é identificado no registo de risco como uma consequência.

A inexistência de um evento e de um risco é retratada pelo vazio nos campos **Risco_Nome** e **Evento_Nome**. No entanto, tanto o risco como o evento têm identificadores a fim de se poder associar a consequência em questão à ausência de evento e risco. O objetivo será não perder informação da **INCM** daí haver um campo para o nível de risco, apesar de este ter sido atribuído na realidade a uma consequência pela organização em causa. Além disso, a consequência é também associada aos respetivos controlos e donos. Toda esta informação estruturada pode ser rastreada a RR1, como se pode verificar na **Figura 18**, para identificar quais os dados da **INCM** que foram usados para esta estruturação, e para fins de validação da mesma.

No que diz respeito ao caso RR2, a ação recomendada foi a de estruturar a informação exposta num risco, já que tínhamos tanto um evento como uma consequência. No entanto, determinou-se que em RR2 tínhamos duas consequências para o evento identificado e não só uma; como tal, temos dois riscos. Pode-se ver na **Figura 18** que tanto os riscos R2 como R3 são rastreáveis a RR2; partilham o mesmo evento mas cada um tem a sua respetiva consequência. Sem mais informação disponível assumiu-se que, para todos os riscos abrangidos pelo caso RR2, o nível de risco, os controlos e os donos de risco são os mesmos.

3.4 Conclusões do Capítulo

No presente capítulo, começou-se por se analisar o caso do *Metro Lisboa* para salientar como o seguimento de um método formal pode fomentar a qualidade da gestão de risco numa organização,

e como não se seguir as recomendações da norma ISO 31000 pode levar a que um plano tenha algumas falhas.

De seguida, estudou-se a ferramenta *registo de riscos*, concluiu-se que se pode testar esta ferramenta para solução do problema e analisou-se como se poderá incorporar um modelo de registo de riscos como um modelo de informação de referência.

Por último, utilizando um método indutivo, procurou-se validar uma solução para o problema do trabalho em mãos. Para fins ilustrativos, foi exibida a aplicação desse processo em dados fornecidos pela **INCM**, apesar de também se terem utilizado os dados nos planos do **IST** e do **LNEC**.

4. Resultados e Discussão

No presente capítulo, pretende-se apresentar o modelo de registo de riscos de referência que se propõe como resultado deste trabalho. Uma vez dada por concluída essa apresentação, partir-se-á para a exemplificação da aplicação de dados da **INCM** no modelo proposto em *excel* e na ferramenta *HoliRisk*.

Seguindo o processo de validação exposto anteriormente, foi possível estruturar riscos de organizações distintas (**INCM, IST** e **LNEC**) num registo de riscos de referência. Nas subsecções **4.2** e **4.3**, pretende-se mostrar o resultado dessa estruturação para dados da **INCM** de modo a alcançar dois objetivos. O primeiro passa por corroborar os resultados expostos na subsecção **4.1**. O segundo passa por explicar os vários conceitos do modelo proposto mediante exemplos da sua aplicação.

Nos Apêndices **B.1. Aplicação do Modelo Proposto aos Dados do IST** e **B.2. Aplicação do Modelo Proposto aos Dados do LNEC**, são já exibidos os resultados finais obtidos via a aplicação deste processo aos dados presentes no plano de gestão de riscos do **IST** e do **LNEC**[17].

Para concluir, ir-se-á proceder a uma discussão sobre os resultados obtidos neste trabalho; que alternativas se poderiam ter seguido e sugestões de melhoria para trabalhos futuros.

4.1 Modelo Proposto

Como se pôde ver no capítulo anterior, a solução do problema foi validada com sucesso. Assim sendo, os próximos parágrafos serão dedicados a explicitar a proposta do registo de riscos de referência para as várias organizações pertencentes ao domínio do problema em mãos. Esse modelo tem cinco entidades como se pode ver na **Figura 19**; por sua vez, cada entidade está associada a uma folha de *excel* (ou a um separador na *HoliRisk* como se poderá ver na subsecção **4.3 – Figura 34**).

Já na **Figura 20**, **Figura 21**, **Figura 22**, **Figura 23** e **Figura 24**, podem-se visualizar os atributos de cada entidade neste modelo de registo de riscos de referência. Opta-se por explicar mais detalhadamente o conceito por detrás de cada atributo nas subsecções **4.2** e **4.3**, onde se recorrerá ao uso de exemplos ilustrativos.

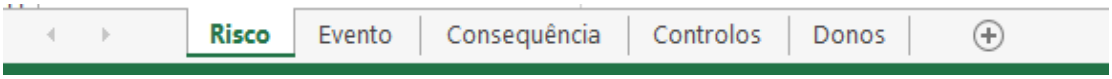

Figura 19 – Folhas de *excel* para cada entidade no modelo proposto

[17] Devido à quantidade de dados presentes no caso da **INCM**, não seria possível apresentar uma versão completa da aplicação do modelo de referência aos mesmos neste documento.

Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Risco_Flags	Legenda de Risco_Flags	Evento_ID	Consequência_ID	Controlo_ID	Dono_ID	Notas do Risco

Figura 20 – Organização da entidade *Risco* no registo de riscos de referência proposto

Evento_ID	Evento_Nome	Evento_Descrição	Likelihood	Unidade de Negócio	Atividade	Evento_Flags	Notas do Evento

Figura 21 – Organização da entidade *Evento* no registo de riscos de referência proposto

Consequência_ID	Consequência_Nome	Consequência_Descrição	Impacto	Consequência_Tipo	ConqEstruturada_Flags	Notas da Consequência

Figura 22 – Organização da entidade *Consequência* no registo de riscos de referência proposto

Controlo_ID	Controlo_Nome	Controlo_Descrição	Controlo_Tipo	Notas dos Controlos

Figura 23 – Organização da entidade *Controlo* no registo de riscos de referência proposto

Dono_ID	Dono_Nome	Dono_Descrição	Notas dos Donos

Figura 24 – Organização da entidade *Dono* no registo de riscos de referência proposto

4.2 Exemplo de Estruturação de Dados em Excel

Na **Figura 25**, **Figura 26**, **Figura 27** e **Figura 28**, podemos analisar como se estruturou a informação referente aos riscos R8, R9, R10 e R11 num registo de riscos em *excel*. A informação nessas figuras encontra-se na folha *Risco* em *excel*. O objetivo das restantes folhas vistas na **Figura 19** é o de fornecer informação mais detalhada sobre a entidade a que se referem, de modo a que cada uma tenha a sua informação organizada independentemente, e também para não sobrecarregar a folha *Risco*.

Na estruturação da entidade *Risco*, o primeiro atributo que surge é o **Risco_ID** que tem a finalidade de identificar cada risco. Em **Risco_Nome**, é apresentado o nome dado ao risco; este nome pode ser: " <*consequência associada ao risco*> devido à ocorrência do <*evento associado ao risco*> ". Os casos em que o campo desse atributo esteja vazio (como se pode ver em R11 na **Figura 25**) correspondem a "não-riscos", isto é, este caso não corresponde a um risco conforme definido na norma ISO 31000 mas sim a um evento ou a uma consequência.

Segue-se o atributo **Nível de Risco** que corresponde ao nível atribuído ao risco pela **INCM** no caso do qual o mesmo foi rastreado. Assim se explica como em R11, que na realidade não é um risco, se exibe um nível de risco; sabe-se então que o evento ou consequência correspondente a R11 (ou RR9 conforme se pode ver em **Rastreio**) foi considerado pela **INCM** como sendo de nível moderado. O atributo seguinte é o de **Rastreio** que, como já mencionado, associa o risco em questão ao "risco" respetivo conforme o relatório da organização estudada.

Por último, cada caso de um possível risco tem associado a si uma *flag* (**Risco_Flags**). Este atributo tem a finalidade de tipificar riscos, o que facilitará a sua organização numa estrutura de informação como a *HoliRisk*. Mais, as *flags* permitem rapidamente obter informação relevante sobre a estruturação do risco a que a mesma se refere. Para o registo de riscos que se concebeu nesta investigação, considerou-se que cada risco seria associado a uma de seis *flags* existentes:

1) **RC** – Risco que se conseguiu estruturar especificamente; área da corrupção e infrações conexas.
2) **RC-Gen** – Risco que foi deduzido com base na informação (estruturação genérica); área da corrupção e infrações conexas.
3) **RD** – Risco que se conseguiu estruturar (específica ou genericamente); não se conseguiu determinar se pertence ou não à área da corrupção e infrações conexas.
4) **OR** – Risco que se conseguiu estruturar (específica ou genericamente); não pertence à área da corrupção e infrações conexas.
5) **N-Cq** – Nestes casos, não existe um risco já que não foi possível a sua estruturação por indeterminação da consequência do evento respetivo.
6) **N-Ev** – Nestes casos, não existe um risco já que não foi possível a sua estruturação por indeterminação do evento que origina a consequência respetiva.

Risco					
Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Risco_Flags	Legenda de Risco_Flags
R8	Insatisfação das áreas requisitantes por fraca qualidade dos materiais	Fraco	RR7	RD	Risco que se conseguiu estruturar (específica ou genericamente); não se conseguiu deduzir se pertence ou não à área da corrupção e infrações conexas
R9	Favorecimento próprio via processo de aquisição incompleto	Moderado	RR8	RC	Risco que se conseguiu estruturar de um modo específico; área da corrupção e infrações conexas
R10	Apropriação indevida de bens via processo de aquisição incompleto	Moderado	RR8	RC-Gen	Risco que só se conseguiu deduzir com base na informação disponível e, consequentemente, está estruturado de um modo genérico; área da corrupção e infrações conexas
R11		Moderado	RR9	N-Cq	Nestes casos, não temos um risco já que não foi possível a sua estruturação por indeterminação da consequência do evento respetivo

Figura 25 – Estruturação da entidade *Risco* em *excel*

Evento						
Evento_ID	Evento_Nome	Evento_Descrição	Unidade de Negócio	Atividade	Evento_Flags	Legenda de Evento_Flags
EV7	Fraca qualidade dos materiais		Compras	Compra	DC	Não se conseguiu apurar o contexto do evento (se se encontra ou não dentro do contexto da corrupção e infrações conexas)
EV8	Processo de aquisição incompleto	Processo de aquisição incompleto (escolha fornecedor, solicitação de cotação, análise de propostas, justificação da seleção da proposta aceite, nota de encomenda, guia de remessa, receção do bem, fatura)	Compras	Compra	EC	Evento encontra-se dentro do contexto da corrupção e infrações conexas
EV8	Processo de aquisição incompleto	Processo de aquisição incompleto (escolha fornecedor, solicitação de cotação, análise de propostas, justificação da seleção da proposta aceite, nota de encomenda, guia de remessa, receção do bem, fatura)	Compras	Compra	EC	Evento encontra-se dentro do contexto da corrupção e infrações conexas
EV9	Inexistência de formalização atempada de contratos	Inexistência de formalização atempada de contratos entre as partes detalhando as condições de fornecimento dos bens/serviços	Compras	Compra	DC	Não se conseguiu apurar o contexto do evento (se se encontra ou não dentro do contexto da corrupção e infrações conexas)

Figura 26 – Estruturação da entidade *Evento* em *excel*

Na **Figura 26**, podem ser analisados os eventos EV7, EV8 e EV9; eventos que se encontram associados a R8, R9, R10 e R11 (EV8 encontra-se associado a R9 e R10 já que estes riscos partem de um mesmo evento para consequências distintas).

Como se pode verificar nessa mesma figura, na estruturação da entidade *Evento*, o primeiro atributo que surge é também um identificador (**Evento_ID**), tal como se verificou na estruturação da entidade *Risco*.

Em **Evento_Nome**, surge o nome do evento caso este exista efetivamente; e, em **Evento_Descrição**, poder-se-á encontrar uma descrição mais pormenorizada do evento em questão, se tal não for claro a partir do nome do mesmo.

De seguida, apresenta-se a ***Likelihood*** (caso seja identificada pela organização em questão, senão esse campo pode ser ocultado como sucede neste caso) de ocorrência do evento; e também é

apresentada a **Unidade de Negócio** e a **Atividade** em que, de acordo com a organização analisada, podem ocorrer os eventos em questão.

Por último, assim como para a entidade *Risco*, procede-se à tipificação dos vários eventos através do uso de *flags* (**Evento_Flags**). A cada evento no registo de riscos exposto, associou-se uma de três *flags* possíveis:

1) **EC** – Evento encontra-se dentro do contexto da corrupção e infrações conexas;
2) **DC** – Não se conseguiu apurar o contexto do evento (se se encontra ou não dentro do contexto da corrupção e infrações conexas);
3) **Outro** – Evento não se encontra dentro do contexto da corrupção e infrações conexas.

A entidade *Consequência* é composta por seis atributos (na **Figura 27**, um dos atributos encontra-se ocultado). O primeiro atributo é um identificador (**Consequência_ID**), o segundo atributo é o nome dado à consequência em si (caso esta tenha sido determinada) – **Consequência_Nome –** , e o terceiro atributo consiste numa descrição mais pormenorizada da consequência caso se considere ser necessário explicitar mais informação sobre essa mesma consequência (**Consequência_Descrição**).

Já o quarto atributo corresponde ao **Impacto** (caso seja identificado pela organização em causa, senão esse campo pode ser ocultado como sucede neste caso) dessa consequência nos objetivos da organização.

Os dois últimos atributos relacionam-se com a tipificação das consequências segundo crimes identificados no Código Penal Português. A ideia de aplicar este conceito partiu de uma leitura atenta do relatório do plano de gestão de riscos da **INCM**, onde são identificados os crimes que essa organização considera serem os mais relevantes (mas não necessariamente os únicos) no contexto da corrupção e infrações conexas. A listagem desses crimes pode ser estudada no Apêndice **A.3. Código Penal – Crimes de Corrupção e Conexos**.

Assim sendo, decidiu-se incluir esta informação no registo de riscos; tendo daí resultado o atributo **Consequência_Tipo**. Este atributo tem como objetivo informar qual ou quais os crimes referentes ao Código Penal que estão relacionados a uma determinada consequência. No entanto, este campo pode não conter informação em casos nos quais não exista uma consequência ou em consequência aonde simplesmente não foi possível determinar que crime poderia estar a ser cometido na eventual ocorrência da mesma.

A **ConqEstruturada_Flags** permite tipificar as consequências mediante a sua identificação conforme o Código Penal, isto é, se foi possível identificar crimes do Código Penal nessa consequência ou não.

Consequência				
Consequência_ID	Consequência_Nome	Consequência_Descrição	Consequência_Tipo	ConqEstruturada_Flags
CQ6	Insatisfação das áreas requisitantes			Não
CQ3	Favorecimento próprio		Recebimento indevido de vantagem	Sim
CQ7	Apropriação indevida de bens		Peculato	Sim
CQ8				Não

Figura 27 – Estruturação da entidade *Consequência* em *excel*

Para finalizar, é necessário exibir também exemplos da estruturação dos controlos e dos donos dos riscos. Os quatro riscos exibidos na **Figura 25** têm os controlos e donos com os identificadores que surgem na **Figura 28**. No entanto, não é visível mais informação acerca dos mesmos nessa mesma figura. Considerou-se que acrescentar um atributo que exibisse os nomes dos controlos e dos donos seria contraproducente, já que um campo para tal atributo poderia ter uma dimensão significativa.

Assim sendo, a título de exemplo, ir-se-ão analisar alguns controlos e donos identificados nas folhas de *excel* que contêm exclusivamente informação sobre cada controlo e sobre cada dono de risco. Por outro lado, o campo **Notas do Risco** é um espaço de comentário livre caso se pretendam deixar algumas notas relevantes sobre o risco em questão; todas as entidades possuem um atributo conceptualmente semelhante a este (ex.: **Notas do Evento**).

Controlos & Donos		*Notas do Risco*
Controlo_ID	Dono_ID	
CONT2; CONT4	DONO1; DONO21	
CONT1; CONT2; CONT9; CONT12; CONT13	DONO1; DONO2; DONO21	
CONT1; CONT2; CONT9; CONT12; CONT13	DONO1; DONO2; DONO21	
CONT1; CONT2; CONT4; CONT8; CONT9; CONT11; CONT12; CONT13	DONO1	

Figura 28 – Estruturação das entidades *Controlos* e *Donos* em *excel*

Na **Figura 29**, podemos analisar os controlos identificados com o **Controlo_ID** de CONT1, CONT2, CONT3 e CONT4. Esses controlos têm um nome que é especificado em **Controlo_Nome** e, se necessário, uma descrição mais detalhada dos mesmos em **Controlo_Descrição**.

Com o atributo **Controlo_Tipo**, procura-se tipificar cada controlo consoante a informação presente no glossário[18] de combate à corrupção da *Transparency International* (ver Apêndice **A.4. Glossário de Soluções para Combate à Corrupção (*Transparency International*)**), uma organização não-governamental de combate à corrupção.

Por último, no campo **Notas dos Controlos**, é possível deixar comentários sobre o respetivo controlo.

Relativamente à estruturação dos donos de risco, a **Figura 30** fornece um exemplo de como a mesma funciona para essa entidade. O primeiro atributo é um identificador (**Dono_ID**), como o é de resto para as outras entidades deste modelo. Segue-se o atributo **Dono_Nome**. Segundo a norma ISO 31000, tanto uma pessoa como uma entidade podem ser consideradas como donos de riscos. No entanto, no caso da **INCM**, os donos de risco eram sempre entidades. Nesses casos, o nome que surge no campo do atributo **Dono_Nome** é a abreviatura do departamento/seção da **INCM** que esta determinou como sendo o dono do risco; enquanto que, no campo do atributo **Dono_Descrição**, surge a denominação dessa mesma entidade. Se os donos fossem indivíduos, poder-se-ia colocar o nome do dono em **Dono_Nome** e a sua função na organização em **Dono_Descrição**. O atributo final é **Notas dos Donos**, que funciona como o campo de comentário livre para esta entidade. No exemplo da **Figura 30**, este atributo reveste-se de particular importância no entendimento dos donos de risco referidos. Os comentários presentes nesses campos fornecem informação que permite inferir porque é que o campo **Dono_Descrição** está vazio para o DONO15 (o relatório da **INCM** não menciona ARH), e porque se decidiu não colocar qualquer denominação em **Dono_Nome.**

Controlo_ID	Controlo_Nome	Controlo_Descrição	Controlo_Tipo	*Notas dos Controlos*
CONT1	Regulamento de Aquisições		Conformidade	
CONT2	C.C.P. - Código dos Contratos Públicos		Conformidade	
CONT3	Plano Económico e Financeiro (PEF)		??	
CONT4	Processo de apoio definido no âmbito da qualidade - Compras		Acesso a informação	

Figura 29 – Informação sobre os controlos CONT1, CONT2, CONT3 e CONT4

[18] Este glossário encontra-se disponível em: https://www.transparency.org/glossary.

Dono_ID	Dono_Nome	Dono_Descrição	*Notas dos Donos*
DONO1	DCP	Direção de Compras	
DONO2	DFI	Direção Financeira	
DONO15	ARH		Surge no Risk Register original mas não é mencionado no plano de gestão de riscos
DONO28	??	Comissão de trabalhadores	Não é mencionado como sendo departamentos específicos no plano de gestão de riscos

Figura 30 – Informação sobre os donos de risco DONO1, DONO2, DONO15 e DONO26

4.3 Exemplo de Estruturação de Dados na *HoliRisk*

A gestão de risco tem por objetivo definir e gerir políticas para endereçar riscos presentes nos vários contextos organizacionais. Essa diversidade de contextos possível apresenta-se como um desafio para a gestão de riscos numa organização, pelo que a mesma é geralmente conduzida em *silos* específicos, orientados a atividades distintas. Assim sendo, é comum encontrar-se nas várias organizações uma ideia de risco fragmentada, com diferente vocabulário e parametrizações.

Para colmatar esta necessidade, o grupo de pesquisa IDSS do INESC-ID decidiu desenvolver a *HoliRisk*, uma plataforma flexível e genérica o suficiente, que apresenta uma visão holística, e desenhada tendo em conta as boas-normas da gestão de risco.

Na **Figura 31**, é apresentado o ecrã de gestão de domínios desse *software*. É a partir deste menu que se pode criar um modelo de domínio e documentar a informação sobre os riscos a ele associados. No *Model Designer*, é possível desenhar de raiz um modelo de domínio entidade-associação, isto é, um diagrama onde se associam múltiplas entidades pertencentes ao domínio (e sendo cada entidade composta por um conjunto de atributos).

A **Figura 32** exibe o exemplo do diagrama correspondente ao modelo recomendado, onde se pode verificar a existência das cinco entidades do modelo proposto (*Risco*, *Evento*, *Consequência*, *Controlos* e *Donos*) e as associações entre essas mesmas entidades. No *Model Designer*, pretende-se traduzir a relação entre entidades; por exemplo, um risco pode estar associado a vários controlos e um dono de risco pode estar associado a múltiplos riscos. Mais, conforme já mencionado, cada uma destas entidades é um conjunto de atributos; por exemplo, a entidade *Risco* tem atributos como nome do risco e nível de risco.

Voltando à **Figura 31**, depois de se ter criado um modelo de domínio, pode-se utilizar o *Register* como uma ferramenta para arquivar e organizar os riscos associados a esse mesmo modelo. Através da visualização da **Figura 33** e da **Figura 34**, pode-se ter uma ideia do que consiste o *Register* do *HoliRisk*. É um registo de riscos que permite organizar e filtrar todos os dados desse modelo conforme desejado.

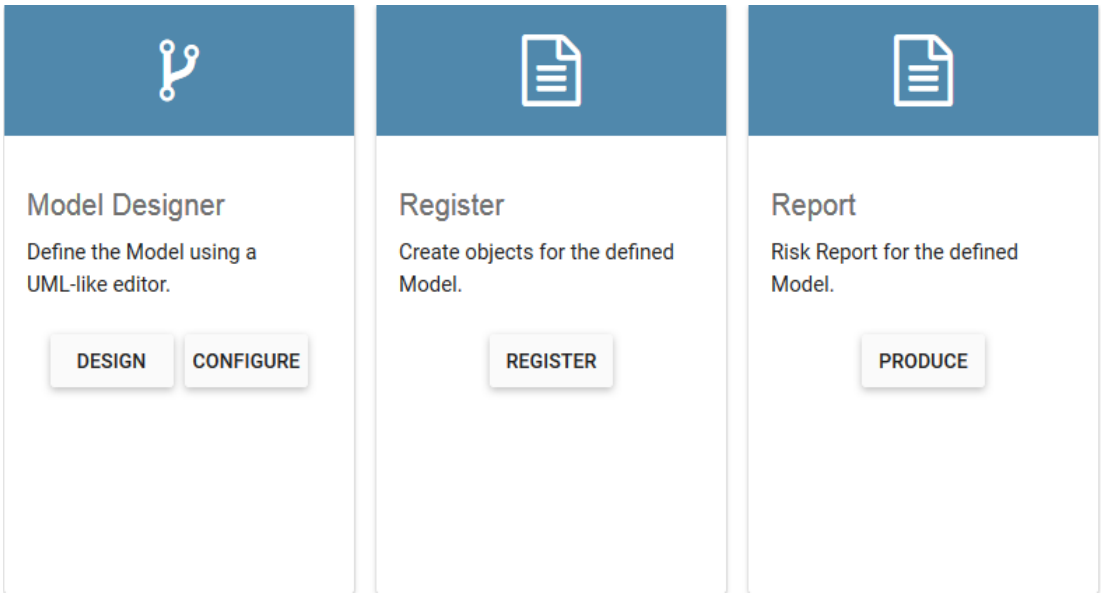

Figura 31 – Ecrã de gestão de domínios na *HoliRisk*

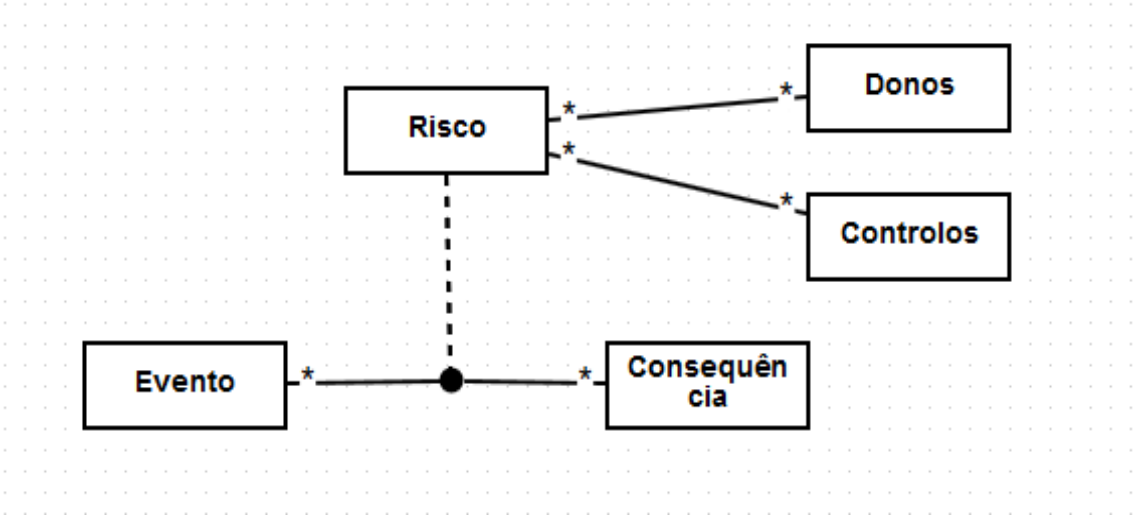

Figura 32 – Modelo de domínio na *HoliRisk*

Figura 33 – Registo de riscos na *Holirisk*

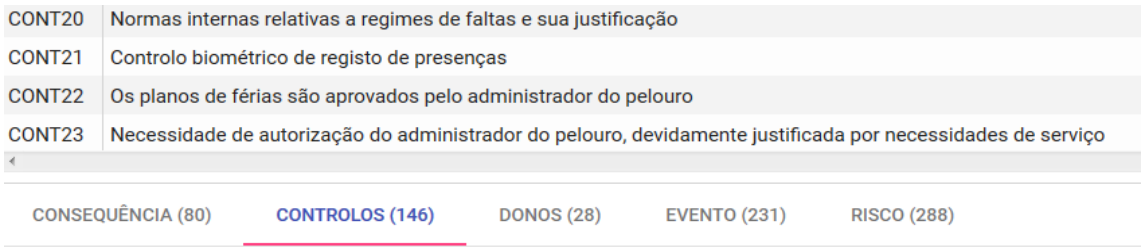

Figura 34 – Rodapé do registo de riscos na *HoliRisk*

Na **Figura 33**, é possível ver que a entidade exibida (*Controlos*) tem quatro atributos visíveis (*Id*, *Name*, *Controlo Descrição* e *Controlo Tipo*). No entanto, apenas três são selecionados para visualização graças ao uso de filtros.

Já na **Figura 34**, podemos ver o rodapé desse *Register*, onde se pode selecionar qual a entidade que se pretende visualizar; para este exemplo, pode-se constatar que a entidade selecionada é a entidade *Controlos*, o que coincide com a **Figura 33**.

No entanto uma das características mais interessantes da *HoliRisk* prende-se, como já foi mencionado neste documento, com a facilidade de, numa estrutura de informação como esta, ter uma tipificação acessível dos riscos.

Na **Figura 35**, pode-se ver um exemplo da aplicação das já mencionadas *flags*; mais concretamente, este exemplo mostra o atributo **Risco_Flags** que pretende tipificar os constituintes da entidade *Risco*. Via ordenação da coluna correspondente ao atributo mencionado, verifica-se que existem quatro riscos com a *flag* OR, correspondente a um risco que não se considera se encontrar no âmbito da corrupção e infrações conexas. Além disso, convém deixar claro que o campo **Risco_Nome** encontra-se vazio para R139, uma vez que neste caso não temos realmente um risco mas ou um evento ou uma consequência. Para auxiliar o utilizador, pode ser exibido também o

campo referente à **Legenda de Risco_Flags**, que indica qual o significado da *flag* associada a um dado risco.

Na **Figura 36**, vê-se como a existência das *flags* N-Cq e N-Ev nos permitem imediatamente verificar se se está na presença de um evento ou de uma consequência sem precisar de se ativar os campos correspondentes a **Evento_Nome** e **Consequência_Nome**. Tal acrescenta valor à experiência do utilizador que analise qualquer registo de riscos.

Para o caso da entidade *Evento*, pode-se ver na **Figura 37** que as *flags* correspondentes a essa entidade (**Evento_Flags**) podem ser ordenadas e analisadas de forma semelhante ao que se viu para a entidade *Risco.*

O mesmo se pode dizer da entidade *Consequência*, como se pode constatar na **Figura 38**. Aqui não temos *flags* no verdadeiro sentido da palavra, mas sim tipos do Código Penal que se considera estarem relacionados com a consequência em questão. Como já foi mencionado, esse atributo denomina-se de **Consequência_Tipo**.

Por último, na entidade *Controlo,* também temos tipos (desta vez retirados do glossário da *Transparency International*) e não propriamente *flags* (ver **Figura 39**). No entanto, o que importa salientar é que existe um atributo, mais concretamente, o atributo **Controlo_Tipo**, que permite tipificar os vários controlos.

R281	Obtenção de benefícios in...	RC	Risco que se conseguiu estruturar de um modo específico; área da corrupção e i...
R282	Concessão de benefícios i...	RC	Risco que se conseguiu estruturar de um modo específico; área da corrupção e i...
R5	Favorecimento próprio de...	OR	Risco que se conseguiu estruturar (específica ou genericamente); não pertence à...
R139		OR	Risco que se conseguiu estruturar (específica ou genericamente); não pertence à...
R145	Concussão devido a ocorr...	OR	Risco que se conseguiu estruturar (específica ou genericamente); não pertence à...
R170	Interrupção ou outro géne...	OR	Risco que se conseguiu estruturar (específica ou genericamente); não pertence à...

Figura 35 – Exemplo de ordenação na *HoliRisk* para o atributo *Risco_Flags*

Id	Name	Risco Flags	Evento Nome	Consequência Nome
R284		N-Cq	Circulação de pessoal n...	
R285		N-Cq	Irregularidades no arma...	
R287		N-Cq	Circulação de pessoal n...	
R1		N-Ev		Favorecimento de terceiros
R34		N-Ev		Existência de conluio entre o...
R81		N-Ev		Incompatibilidades na acumu...

Figura 36 – Exemplo de valor acrescentado da *flag Risco_Flags*

EV225	Irregularidades no estabeleciment...	EC
EV231	Extravio interno/externo da docum...	EC
EV4	Dependência de fornecedores	Outro
EV107	Inexistência de informação de saíd...	Outro

Figura 37 – Exemplo de ordenação na *HoliRisk* para o atributo *Evento_Flags*

CQ62	Furto ou apropriação de b...	Peculato
CQ69	Apropriação de valores	Peculato
CQ60	Utilização indevida de ben...	Peculato de uso
CQ61	Utilização indevida de ben...	Peculato de uso
CQ5	Obtenção de vantagens p...	Peculato; abuso de poder
CQ3	Favorecimento próprio	Recebimento indevido de vantagem
CQ27	Não desconto posterior d...	Recebimento indevido de vantagem

Figura 38 – Exemplo de ordenação na *HoliRisk* para o atributo *Consequência_Tipo*

CONT121	Norma interna sobre Cond...	Conformidade
CONT129	Norma interna sobre comi...	Conformidade
CONT17	Legislação Nacional e/ou ...	Conformidade; convenções
CONT10	Delegação de competências	Prestação de contas
CONT14	Aprovação da aquisição	Prestação de contas
CONT15	Obrigatoriedade de todos ...	Prestação de contas

Figura 39 – Exemplo de ordenação na *HoliRisk* para o atributo *Controlo_Tipo*

4.4 Discussão

Considera-se importante realçar que este modelo de referência proposto não é uma solução ótima para este problema; é sim o resultado de múltiplas iterações até se chegar a um modelo que se considerasse simples o suficiente para o contexto do problema mas contendo os principais conceitos recomendados pela norma ISO 31000. Assim sendo, acredita-se ser possível (em trabalhos futuros

na área de gestão de risco) obter um modelo que se considere mais adequado para as organizações. No entanto, é de se salientar que a solução proposta é para ser tida em conta como referência genérica; tal como recomendado na norma ISO 31000, a organização é encorajada a adaptar a estrutura de gestão de risco ao contexto em que a mesma se insere (por exemplo: inclusão ou exclusão de certas entidades ou atributos expostos no modelo proposto).

Na elaboração do modelo de referência, procuraram-se sempre ter em mente os princípios e recomendações da norma ISO 31000 já que esta é a norma nacional oficial de gestão de risco, e esta norma é genérica o suficiente para aplicação em qualquer domínio. Além disso, a única norma universalmente aceite para gerir riscos no domínio específico da corrupção é a **UNCAC** que, no entanto, é mais focada para aplicação por Estados e/ou partidos políticos. A norma ISO 37001 remete-se apenas à análise de sistemas de combate ao suborno, enquanto que o problema em mãos abrange todo o domínio da corrupção e infrações conexas.

De seguida, analisam-se os atributos do modelo de referência que procuram medir o nível de risco, a *likelihood* de ocorrência de um evento ou o impacto de uma dada consequência nos objetivos de uma organização. Optou por se proceder a uma avaliação qualitativa (em vez de quantitativa) assente em três níveis conceptuais (por exemplo: fraco; moderado; elevado). Considerou-se que, para algumas organizações, pode ser complicado avaliar riscos de modo a determinar a sua posição numa avaliação que estivesse assente em mais do que três níveis (por exemplo: muito fraco, fraco, médio, alto, muito alto); enquanto que uma avaliação quantitativa pode ser ainda mais complicada mediante os fatores sociais associados ao âmbito da corrupção. No entanto, mais uma vez, uma organização é encorajada a adaptar o modelo de modo a que este melhor se adeque às suas necessidades.

Em relação ao atributo **Consequência_Tipo**, é de se salientar que, neste trabalho, apenas foram tidos em conta um conjunto de dez crimes (ver Apêndice **A.3. Código Penal – Crimes de Corrupção e Conexos**); no entanto, poderão existir outros crimes relacionados com corrupção no Código Penal. Além disso, é importante salientar que, de qualquer modo, a aplicação deste atributo pode ser subjetiva mediante as diferentes interpretações que se façam de uma consequência relativamente ao Código Penal.

Em relação ao atributo **Controlo_Tipo** já foram tidos em conta todos os conceitos do glossário da *Transparency Intenational* (ver Apêndice **A.4. Glossário de Soluções para Combate à Corrupção (*Transparency International*)**); no entanto, a sua aplicação também pode ser subjetiva mediante a interpretação que se faça de um dado controlo.

5. Conclusões Gerais e Desenvolvimento Futuro

No presente capítulo, ir-se-ão retirar conclusões gerais sobre o trabalho aqui desenvolvido, serão deixadas algumas recomendações antes de se dar por concluído este documento e, para o concluir, dar-se-ão sugestões para trabalhos futuros que possam ter este mesmo trabalho como ponto de partida.

5.1 Conclusões

Verificando-se a heterogeneidade entre os vários planos de gestão de risco requisitados pelo **CPC** e as falhas do ponto de vista das boas-normas da gestão de risco presentes na maior parte dos mesmos (fruto de não se ter seguido qualquer método formal de gestão de risco), concluiu-se que havia a necessidade de conceber um modelo de informação de referência para as várias organizações Portuguesas.

Após análise do caso prático de um dos planos de gestão de riscos melhor elaborados (o do *Metro Lisboa*), concluiu-se que a aplicação de uma metodologia formal de gestão de risco e a sua concordância com os princípios e recomendações da norma ISO 31000 pode, de facto, auxiliar no combate à corrupção. Assim sendo, e tendo em conta o contexto do problema, propôs-se um modelo conceptualmente semelhante ao da **Figura 10**. Através de um processo assente em três passos, conseguiu-se aplicar o modelo proposto aos dados reais de três organizações distintas (**INCM**, **IST** e **LNEC**), e assim validar-se a solução do problema.

Mediante a estruturação bem-sucedida desses casos práticos em duas estruturas de informação distintas (*excel* e *HoliRisk*), concluiu-se também que a solução proposta (ver aplicação da mesma para *excel* na **Figura 20**, **Figura 21**, **Figura 22**, **Figura 23** e **Figura 24**) é flexível, ou seja, o modelo de referência é aplicável em estruturas de informação distintas.

5.2 Lições e Recomendações

Apesar do modelo de domínio ser o principal resultado deste trabalho, é relevante sublinhar o processo utilizado para validação do mesmo. Esse método de três passos foi utilizado para verificar a possibilidade de transferência de dados reais de algumas organizações para o modelo sugerido. Com a validação do modelo, constatou-se que este método é um processo de gestão de risco que uma organização pode usar, em complemento com o modelo proposto, caso esta assim o entenda. Aliás, neste momento, a **INCM** encontra-se a utilizar este processo para implementar o modelo proposto no seu plano de gestão de riscos, o que corrobora a sua utilidade.

Importa então discutir o quão adequado é esse processo. Os passos 1 e 3 do mesmo parecem ser lineares; o primeiro passo consiste em identificar cada caso que seja considerado *risco* pela organização analisada (atribuindo a cada caso um código), e o terceiro consiste na aplicação do

modelo indicado. Já o passo 2 é mais complexo, pois é o passo em que se define como se transitará da estruturação de informação consoante o modelo da organização estudada para a estruturação da mesma informação (é importante não se perder informação) consoante o modelo aqui sugerido. Há casos que podem ser abertos a interpretação (por exemplo, não se consegue determinar se se está perante um evento ou uma consequência) pelo que a existência de um campo de comentário se reveste de particular importância na fundamentação das escolhas tomadas. O campo de *ação recomendada* pode ser útil para uma organização definir se é necessário obter mais informação sobre um certo caso, mas o mesmo pode ser adaptado à realidade da organização que utilize o processo.

Avançando para o modelo proposto, as *flags* concebidas para este modelo de referência pretendem acrescentar valor à gestão de risco numa organização, no entanto, não são consideradas como essenciais ao modelo. Assim sendo, embora o seu uso seja recomendado para uma melhor documentação da informação, também estas *flags* podem ser adaptadas por uma organização. Isto é, as *flags* exibidas neste capítulo pretendem ser um guia, um exemplo de como o uso de atributos conceptualmente semelhantes podem acrescentar valor à gestão de risco sem um aumento significativo da sua complexidade.

Os atributos **Consequência_Tipo** e **Controlo_Tipo** podem não ser de implementação linear numa organização. No caso do primeiro, a sua associação a crimes do Código Penal Português pode tornar a sua aplicação subjetiva; isto é, dois decisores podem ter opiniões distintas sobre se uma dada consequência está ou não associada a um determinado crime previsto no Código Penal. Recomenda-se então uma colaboração com o departamento jurídico (sempre que aplicável) para a correta apreciação das consequências previstas. No caso do segundo, uma vez que não é aplicada qualquer legislação, pode-se aceitar alguma subjetividade; no entanto, espera-se que os controlos sejam discutidos por múltiplos decisores a fim de se obter a melhor interpretação possível do controlo mediante o glossário da *Transparency International*.

Para sumarizar a utilidade deste modelo, é de se salientar a maior homogeneidade que existiria entre os planos de gestão de risco das várias organizações caso este modelo fosse seguido como referência pelas mesmas. Mas, mais do que isso, a principal vantagem da implementação deste modelo numa organização seria a sua conformidade com as boas-normas de gestão de risco; assim como a sua aplicabilidade em qualquer organização, em qualquer estrutura de informação, e no contexto mais específico da corrupção e infrações conexas, assegurando um maior valor acrescentado à gestão de risco na organização.

5.3 Trabalho Futuro

Este trabalho é recomendado como ponto de partida para futuros trabalhos sobre conceção de modelos de informação não só na temática da corrupção e infrações conexas mas em outros *silos*. Tal é possível já que este modelo é baseado em conceitos da norma ISO 31000, conceitos genéricos aplicáveis a qualquer indústria. Os únicos atributos do modelo que são mais específicos ao contexto

deste problema são as *flags* que foram criadas para acrescentar valor a um modelo no domínio da corrupção.

Mais, na subsecção **2.4**, é feita uma breve análise sobre corrupção em indústrias distintas; pelo que essa análise pode ser um ponto de partida para a conceção de um modelo mais específico para corrupção numa dada indústria (a solução deste trabalho é aplicável de modo geral a todas as indústrias).

Por último, caso se pretenda um plano de gestão de riscos mais focado no fenómeno do suborno, será possível iterar um modelo tendo em conta a futura norma ISO 37001 de combate ao suborno (ver subsecção **2.5**).

6. Referências Bibliográficas

[1] Recomendação do CPC de 1 de Julho de 2009 sobre *planos de gestão de riscos de corrupção e infrações conexas*. Conselho de Prevenção da Corrupção. Lisboa.

[2] Conselho de Prevenção da Corrupção. (2015). *Prevenir a corrupção no Setor Público: Uma experiência de 5 anos.* Maia, A.J. Lisboa.

[3] Association of Certified Fraud Examiners. (2014). *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study.* ACFE. Austin, Texas.

[4] ISO 31000:2009. *Risk management – Principles and guidelines.* International Organization for Standardization. Genève.

[5] ISO Guide 73:2009. *Risk management – Vocabulary.* International Organization for Standardization. Genève.

[6] ISO 31010:2009. *Risk management – Risk assessment techniques.* International Organization for Standardization. Genève.

[7] United Nations' Office on Drugs and Crime. (2004). *United Nations Convention against Corruption.* UNODC. Vienna.

[8] Nordin, R.M., Takim, R., Nawawi, A.H. (2013). Behavioral Factors of Corruption in the Construction Industry. *Procedia – Social and Behavioral Sciences.* **105:** 64-74.

[9] Ernst & Young. (2012). *Managing bribery and corruption risks in the construction and infrastructure industry.* EY.

[10] Ernst & Young. (2014). *Managing bribery and corruption risks in the oil and gas industry.* EY.

[11] Ernst & Young. (2013). *Managing bribery and corruption risk in the life sciences industry.* EY.

[12] Ernst & Young. (2013). *Managing bribery and corruption risks in the mining and metals industry.* EY.

[13] Institute of Risk Management, Transparency International UK. (2016). *Bribery risk guide*. IRM, TI-UK. London

[14] International Organization for Standardization. (2015). *ISO 37001 anti-bribery management systems standard: FAQS – Summary.* ISO. Genève.

[15] Metro Lisboa. (2014). *Plano de Prevenção de Riscos de Corrupção e Infrações Conexas.* ML. Lisboa.

[16] Lyytinen, Kalle. (2011). MIS: the urge to control and the control of illusions – towards a dialectic. *Journal of Information Technology.* **26:** 268-270.

A. Apêndices Gerais

A.1. ISO 31000 – Os Onze Princípios Básicos em Inglês

1. **Risk management creates and protects value**: Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.
2. **Risk management is an integral part of all organizational processes**: Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.
3. **Risk management is part of decision making**; Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action
4. **Risk management explicitly addresses uncertainty**: The nature of that uncertainty, and how it can be addressed.
5. **Risk management is systematic, structured and timely**: A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
6. **Risk management is based on the best available information**: The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision-makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.
7. **Risk management is tailored**: Risk management is aligned with the organization’s external and internal context and risk profile.
8. **Risk management takes human and cultural factors into account**: Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.
9. **Risk management is transparent and inclusive**: Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
10. **Risk management is dynamic, iterative and responsive to change**: As external and internal events occur, context and knowledge change, monitoring and review take place, new risks

emerge, some change, and others disappear. Therefore, risk management continually senses and responds to change.

11. **Risk management facilitates continual improvement of the organization**: Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

A.2. Lista de Ferramentas e Técnicas para um Processo de Apreciação de Risco

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1)] Strongly applicable.

[2)] Not applicable.

[3)] Applicable.

Figura 40 – Lista de ferramentas e técnicas para apreciação de riscos (Fonte: [6])

A.3. Código Penal – Crimes de Corrupção e Conexos

- **Recebimento indevido de vantagem:**
  - O funcionário que, no exercício das suas funções, aceita uma vantagem patrimonial (ou não patrimonial) que não lhe seja devida. O funcionário aceita uma vantagem patrimonial (ou não patrimonial) para um ato (ou omissão) contrário aos deveres da função que ocupa (p.p. artigo 372.º do Código Penal).
- **Corrupção passiva por ato lícito:**
  - O funcionário aceita uma vantagem patrimonial (ou não patrimonial) para um ato (ou omissão) não contrário aos deveres da função que ocupa (p.p artigo 373.º do Código Penal).
- **Corrupção ativa:**
  - Quando alguém der ou prometer uma vantagem patrimonial (ou não patrimonial) a um funcionário (p.p. artigo 374.º do Código Penal).
- **Tráfico de influência:**
  - Quando alguém solicitar ou aceitar vantagens (patrimoniais ou não) para abusar da sua influência (p.p. artigo 335.º do Código Penal).
- **Peculato:**
  - Quando um funcionário de uma forma ilegítima se apropriar ou aceitar algo que lhe seja acessível, devido às funções que ocupa (p.p. artigo 375.º do Código Penal).
- **Peculato de uso:**
  - Quando um funcionário fizer uso de veículos ou outras coisas móveis, de um modo distinto àquele que originalmente se destinavam, e que lhe sejam acessíveis devido às funções que ocupa (p.p. artigo 376.º do Código Penal).
- **Participação económica em negócio:**
  - Quando um funcionário devido às funções que ocupa, nomeadamente administrar ou fiscalizar obtenha uma participação económica ilícita em negócio jurídico ou interesses patrimoniais (p. p. artigo 377.º do Código Penal).
- **Concussão:**
  - Quando um funcionário no exercício das suas funções receber vantagem patrimonial indevida, decorrente de aproveitamento ou indução em erro (p.p. artigo 379.º do Código Penal).
- **Abuso de poder:**
  - Quando um funcionário (excluindo os casos anteriores) abusar de poderes intrínsecos à sua função com intenção de obter benefícios ilegítimos (p.p. artigo 382.º do Código Penal).

- **Violação de segredo por funcionário:**
    - Quando um funcionário, sem a conveniente autorização, revelar informações, que tenha tido conhecimento com a intenção de obter benefícios (p.p. artigo 383.º do Código Penal).

A.4. Glossário de Soluções para Combate à Corrupção (*Transparency International*)[19]

- **Acesso à informação (*access to information*):**
  - O direito legal – normalmente via legislação para liberdade de informação – de aceder a dados-chave do governo e de qualquer outro órgão público com base no conceito de que cidadãos podem obter informação que está na posse do Estado.
- **Prestação de contas (*accountability*):**
  - O conceito que dita que indivíduos e organizações (públicas, privadas e sociedades civis) são responsáveis por reportar as suas atividades e por exercerem adequadamente os seus poderes. Também inclui a responsabilidade por dinheiro ou outras propriedades que lhe tenham sido confiadas.
- **Recuperação de ativos (*asset recovery*):**
  - Processo legal através do qual um país, governo e/ou seus cidadãos recuperam ativos que lhes foram roubados sob outra jurisdição devido a um fenómeno de corrupção.
- **Auditorias (*audit*):**
  - Um exame interno ou externo de uma organização no que diz respeito às suas contas, processos, funções e performance, a fim de produzir uma avaliação credível e independente, e que garanta a conformidade com as devidas leis e regulações.
- **Troca automática de informação (*Automatic Exchange of Information (AIE)*):**
  - Quando as autoridades fiscais de múltiplos Estados partilham informação financeira relacionada com todos os tipos de riqueza (inclusive ativos fixos como casa ou terrenos) e atividade taxável (e.g. dividendos, juros, salários, pensões, reembolsos, etc.) de forma periódica e automática. Neste sistema, informação é recolhida no país onde ocorre tal atividade ou onde existe tal riqueza, e é partilhada com o país que deve taxas sem ser necessário um requerimento formal.
- **Código de conduta (*code of conduct*):**
  - Declaração de princípios e valores que estabelece um conjunto de expetativas e normas para como uma organização ou corpo governamental irá conduzir suas atividades.
- **Conformidade (*compliance*):**
  - Refere-se a procedimentos, sistemas ou departamentos dentro de agências públicas ou empresas que asseguram a conformidade das atividades financeiras,

[19] Todos os termos e definições utilizados neste apêndice constituem traduções livres das respetivas versões em inglês.

operacionais e legais com as leis, regras, normas, regulações e normas em vigor, e com expetativas públicas.

- **Convenções (*conventions*):**
  - Acordos regionais e/ou internacionais assinados ou ratificados por vários Estados que estabelecem regras, leis e normas em assuntos que necessitem de uma abordagem comum para uma cooperação efetiva entre todos os envolvidos.
- **Governança corporativa (*corporate governance*):**
  - Procedimentos e processos para como organizações do setor privado são conduzidas, controladas e geridas, incluindo as relações entre, responsabilidades de e expetativas legítimas entre diferentes *stakeholders*.
- **Relatórios de país-por-país (*country-by-country reporting*):**
  - Quando companhias multinacionais produzem certos dados financeiros desagregados por país e para cada país em que operem. Tais dados incluem vendas e compras dentro da multinacional e externamente, lucros, perdas, número de empregados e respetivos custos, impostos pagos e a pagar, e sumários de ativos e passivos.
- **Exclusão (*debarment*):**
  - Procedimento onde organizações e indivíduos são excluídos de participarem em ou organizarem projetos. Governos e agências multilaterais usam este procedimento para gastar negócios publicamente, assim como *NGO's*, países ou indivíduos que sejam determinados culpados de comportamento não ético e fora-da-lei.
- **Divulgação (*disclosure*):**
  - Provisão de informação como requerido por lei ou em boa-fé, olhando a atividades de privados ou públicos. Informação pode incluir os ativos de um candidato político, os relatórios financeiros de uma empresa, os dadores numa *NGO* ou as acusações de um *whistleblower*.
- **Reforço de diligências (*enhanced due diligence*):**
  - O termo usado para se referir a medidas de lavagem de dinheiro "Know Your Customer" que incluem validação e documentação por terceiros e que se aplica a situações que envolvam clientes com maior risco ou indivíduos politicamente expostos.
- **Ética (*ethics*):**
  - Baseada em valores e normas básicas, é um conjunto de normas de conduta num governo, em empresas ou na sociedade, usada para guiar em decisões, escolhas e ações.

- **Governança (*Governance*):**
    - Um conceito que vai para além da noção tradicional de governo para se concentrar antes nas relações entre líderes, instituições públicas e cidadãos, incluindo os processos pelos quais são tomadas e implementadas decisões. O termo pode também ser aplicado a empresas e *NGO's*. 'Boa' governança é caraterizada por ser participativa, responsabilizável, transparente, eficiente, responsiva e, inclusive, respeitando o Estado de Direito e minimizando oportunidades para corrupção.
- **Integridade (*integrity*):**
    - Comportamentos e ações consistentes com um conjunto de princípios éticos e morais, abraçados por indivíduos e instituições, criando assim uma barreira para a corrupção.
- ***Know Your Customer (KYC)*:**
    - Um termo usado para descrever um conjunto de medidas relacionadas com lavagem de dinheiro que são normalmente exigidas por lei e que são empregadas por bancos e outros serviços financeiros a fim de documentar a verdadeira identidade de um cliente assim como a sua fonte de rendimentos de modo a que se possa assegurar a sua legitimidade. Esta informação é compilada e guardada num "perfil" que é atualizado periodicamente. Atividade relacionada com uma dada conta é comparado com o "perfil" *KYC* a fim de identificar atividade suspeita de se encontrar no contexto de lavagem de dinheiro.
- **Assistência jurídica mútua (*Mutual Legal Assistance (MLA)*):**
    - O processo formal de cooperação entre múltiplas jurisdições, por exemplo em casos de lavagem de dinheiro, recuperação de ativos e evasão fiscal. Através desta cooperação, que é normalmente explicitada através de um tratado, um Estado pode pedir e receber assistência na recolha de informação e de provas vindas de fontes púbicas e privadas para uso em investigações e acusações oficiais.
- **Sistemas de integridade nacional (*national integrity systems*):**
    - Uma abordagem holística para analisar tanto o alcance como as causas da corrupção num determinado país olhando para um sistema de pilares institucionais que formam uma sociedade, incluindo a sociedade executiva, legisladora, judiciária, civil e o setor de negócios. Desenvolvida pela *Transparency International*, esta estrutura é útil para avaliar os pontos institucionais fortes e fracos de um país e desenvolver uma estratégia de combate à corrupção.
- **Fiscalização (*oversight*):**
    - O processo de monitorizar e investigar de forma independente – interna ou externamente – as operações e atividades de uma agência governamental,

empresa ou sociedade civil para assegurar a prestação de contas (*accountability*) e o uso eficiente de recursos.

- **Pactos (*pacts*):**
  - Acordo voluntário entre partes distintas (i.e. negócios, agências governamentais) para obediência formal a "regras do jogo" mutuamente acordadas, incluindo a recusa de realizar subornos e a promessa de respeitar os direitos humanos.
- **Vontade política (*political will*):**
  - Demonstração e compromisso por líderes políticos em enfrentar desafios sociais ou em cumprir uma promessa política, como combater a corrupção ou um aumento da participação política, através do uso das políticas reformatórias adequadas.
- **Estado de Direito (*Rule of Law*):**
  - Sistemas políticos e legais, estruturas e práticas que condicionam as ações de um governo para proteção dos direitos e liberdades dos cidadãos, manter lei e ordem, e encorajar o funcionamento eficaz do país.
- **Transparência (*Transparency*):**
  - Característica de governos, empresas, organizações e indivíduos terem abertamente a seu dispor informação, regras, planos, processos e ações divulgadas. Por princípio, oficiais públicos, gestores e diretores de empresas e organizações têm o dever de agir visivelmente, com previsibilidade e de modo compreensível a fim de promover participação e prestação de contas (*accountability*) e permitir a terceiros a fácil perceção de quais as ações a serem efetuadas.
- ***Whistleblowing*:**
  - Fazer uma divulgação de interesse público, quer se seja um empregado, diretor ou externo, numa tentativa de revelar negligência ou abusos nas atividades de uma dada organização, corpo governamental ou empresa (ou um dos seus parceiros de negócios) que ameace o interesse público, a sua integridade e reputação. O termo na língua inglesa é visto de modo maioritariamente positivo apesar de muitas línguas não terem esse mesmo conceito quando se usa esta mesma conotação.

B. Aplicações do Modelo de Referência

B.1. Aplicação do Modelo Proposto aos Dados do IST

Risco					Evento	Consequência	Controlos & Donos	
Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Risco_Flags	Evento_ID	Consequência_ID	Controlo_ID	Dono_ID
R1	Erros na emissão de meios de pagamento devido a preenchimento manual de cheques	Moderado	RR1	RD	EV1	CQ1	CONT1; CONT2; CONT3	DONO21; DONO24
R2	Erros na emissão de meios de pagamento devido a processamento de transferências bancárias	Moderado	RR1	RD	EV2	CQ1	CONT1; CONT2; CONT3	DONO21; DONO24
R3		Fraco	RR2	N-Cq	EV3	CQ2	CONT4; CONT5; CONT6; CONT7	DONO21; DONO22
R4	Aquisição de bens fora do âmbito do fundo de maneio devido a urgência	Fraco	RR3	RD	EV4	CQ3	CONT4; CONT5; CONT6; CONT7	DONO21; DONO22
R5		Moderado	RR4	N-Cq	EV5	CQ4	CONT8; CONT9	DONO21; DONO23
R6		Moderado	RR5	N-Cq	EV6	CQ5	CONT10; CONT11	DONO21; DONO23
R7		Fraco	RR6	N-Ev	EV7	CQ6	CONT12	DONO15; DONO21; DONO25; DONO48
R8	Evitação do concurso público devido a repartição da contratação e do respetivo valor	Fraco	RR7	RC	EV8	CQ7	CONT13	DONO49

R9	Favorecimento de fornecedores devido às especificações do produto estarem dirigidas a um determinado fornecedor	Fraco	RR8	RC	EV9	CQ8	CONT14	DONO50
R10		Fraco	RR9	N-Ev	EV10	CQ9	CONT15	DONO15; DONO49; DONO51
R11		Fraco	RR10	N-Ev	EV11	CQ10	CONT15	DONO15; DONO49; DONO51
R12		Fraco	RR11	N-Ev	EV12	CQ11	CONT15	DONO15; DONO49; DONO51
R13		Fraco	RR12	N-Ev	EV13	CQ12	CONT15	DONO15; DONO49; DONO51
R14		Fraco	RR13	RD	EV14	CQ13	CONT16	DONO15; DONO49; DONO51
R15	Benefício de terceiros devido a definição de cláusulas jurídas e técnicas	Fraco	RR14	RD	EV15	CQ14	CONT17	DONO15; DONO49; DONO51
R16		Fraco	RR15	N-Cq	EV16	CQ15	CONT18	DONO15; DONO49; DONO51
R17		Fraco	RR16	RD	EV17	CQ16	CONT18; CONT19	DONO15; DONO49; DONO51
R18	Ausência de inspeção ou de ato que certifique as quantidades e/ou a qualidade dos bens e serviços, antes da emissão da ordem de pagamento	Fraco	RR17	RD	EV18	CQ17	CONT20	DONO15; DONO49; DONO52; DONO53

R19		Fraco	RR18	N-Ev	EV19	CQ18	CONT21; CONT22	DONO26
R20		Fraco	RR19	N-Cq	EV20	CQ19	CONT21; CONT22	DONO26
R21		Fraco	RR20	N-Cq	EV21	CQ20	CONT23; CONT24; CONT25	DONO26; DONO54
R22		Moderado	RR21	N-Cq	EV22	CQ21	CONT26	DONO55
R23		Moderado	RR22	N-Ev	EV23	CQ22	CONT27	DONO42; DONO53
R24	Lançamento de uma nota para favorecer/prejudicar um aluno	Moderado	RR23	RC-Gen	EV24	CQ23	CONT28	DONO42; DONO53
R25		Fraco	RR24	N-Cq	EV25	CQ24	CONT29; CONT30	DONO42; DONO53
R26		Fraco	RR24	N-Cq	EV26	CQ25		
R27	Favorecimento de candidatos devido a divulgação de informação sobre os procedimentos de avaliação	Fraco	RR25	RC	EV27	CQ26	CONT31; CONT32; CONT33; CONT34; CONT35; CONT36	DONO1; DONO7; DONO14; DONO56
R28	Favorecimento de candidatos devido a não consideração do incumprimento de requisitos	Fraco	RR26	RC	EV28	CQ27	CONT31; CONT32; CONT33; CONT34; CONT35; CONT36	DONO1; DONO7; DONO14; DONO56
R29		Fraco	RR27	N-Cq	EV29	CQ28	CONT37; CONT38	DONO14
R30		Fraco	RR28	N-Ev	EV30	CQ29	CONT39; CONT40; CONT41; CONT42	DONO14
R31		Fraco	RR29	N-Ev	EV31	CQ30	CONT39; CONT40; CONT41; CONT42	DONO14

Evento_ID	Evento_Nome	Evento_Descrição	Likelihood	Unidade de Negócio	Atividade	Evento_Flags
EV1	Preenchimento manual de cheques		Fraco	Área Financeira e Contabilística	Pagamento de despesa	DC
EV2	Processamento de transferências bancárias		Fraco	Área Financeira e Contabilística	Pagamento de despesa	DC
EV3	Má utilização da verba atribuída		Fraco	Área Financeira e Contabilística	Processo de Fundo de Maneio	EC
EV4	Urgência		Fraco	Área Financeira e Contabilística	Processo de Fundo de Maneio	DC
EV5	Não registo da receita e emissão de respetiva fatura		Fraco	Área Financeira e Contabilística	Processamento de receita	EC
EV6	Atraso na cobrança da dívida		Fraco	Área Financeira e Contabilística	Processamento de receita	EC
EV7			Fraco	Aquisições de bens e serviçoes/Contratação Pública	Processo de aquisição por ajuste direto	EC
EV8	Repartição da contratação e do respetivo valor		Fraco	Aquisições de bens e serviçoes/Contratação Pública	Fase Pré-Contratual/Escolha dos procedimentos	EC
EV9	As especificações do produto estarem dirigidas a um determinado fornecedor		Fraco	Contratação Pública	Fase Pré-Contratual/Definição de especificações	EC
EV10			Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	EC

EV11			Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	EC
EV12			Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	EC
EV13			Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	EC
EV14	Fracionamento de despesa		Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	DC
EV15	Definição de cláusulas jurídicas e técnicas		Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	DC
EV16	Execução de trabalhos a mais sem devida autorização		Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	EC
EV17	Incumprimento injustificado de prazos		Fraco	Contratação Pública	Aquisições no âmbito da Área de apoio geral e Procedimentos de contratação e do controlo de execução do contrato	DC

EV18	Ausência de inspeção de quantidades e/ou qualidade dos bens e serviços, antes da emissão da ordem de pagamento		Fraco	Contratação Pública	Geral	DC
EV19			Fraco	Património	Gestão Patrimonial	EC
EV20	Dificuldade no controle de bens	Dificuldade no controle de bens (bens que não são etiquetados, empréstimos/cedência de bens não autorizados, abates indevidos)	Fraco	Património	Gestão Patrimonial	EC
EV21	Fragilidades a nível de controlo do inventário do economato e do património		Moderado	Património	Gestão do Património em salas de aula	EC
EV22	Inserção e alteração incorreta de informação dos processos no Fénix		Fraco	Alunos	Registo Académico	EC
EV23			Fraco	Alunos	Registo Académico	EC
EV24	Lançamento fraudulento de uma nota		Fraco	Alunos	Registo Académico	EC
EV25	Lançamento de um pagamento de propinas sem a realização do mesmo		Fraco	Alunos	Emissão de recibos; Controlo de pagamentos de propinas	EC

EV26	Lançamento de um pagamento de propinas noutro processo		Fraco	Alunos	Emissão de recibos; Controlo de pagamentos de propinas	EC
EV27	Divulgação de informação sobre os procedimentos de avaliação		Fraco	Recursos Humanos	Recrutamento por procedimento concursal	EC
EV28	Não consideração do incumprimento de requisitos		Fraco	Recursos Humanos	Recrutamento por procedimento concursal	EC
EV29	Processamento de vencimentos e descontos inexato ou alterado		Fraco	Recursos Humanos	Processamento de vencimentos	EC
EV30			Fraco	Recursos Humanos	Informação/documentos confidenciais	EC
EV31			Fraco	Recursos Humanos	Informação/documentos confidenciais	EC

Consequência_ID	Consequência_Nome	Consequência_Descrição	Impacto	Consequência_Tipo	ConqEstruturada_Flags
CQ1	Erros na emissão de meios de pagamento		Moderado	Tráfico de influência	Sim
CQ2			Moderado		Não
CQ3	Aquisição de bens fora do âmbito do fundo de maneio		Moderado	Recebimento indevido de vantagem	Sim
CQ4			Moderado		Não
CQ5			Moderado		Não
CQ6	Favorecimento de fornecedores (aquisição por ajuste direto)		Moderado	Peculato; abuso de poder	Sim

CQ7	Evitação do concurso público		Fraco	Tráfico de influência	Sim
CQ8	Favorecimento de fornecedores (especificações do produto)		Fraco	Recebimento indevido de vantagem	Sim
CQ9	Favorecimento de fornecedores (aquisições na área de apoio geral)		Elevado	Recebimento indevido de vantagem	Sim
CQ10	Corrupção passiva para ato ilícito		Elevado	Corrupção passiva para ato ilícito	Sim
CQ11	Participação económica em negócio		Elevado	Participação económica em negócio	Sim
CQ12	Tráfico de influência		Elevado	Tráfico de influência	Sim
CQ13			Elevado		Não
CQ14	Benefício de terceiros		Elevado		Não
CQ15			Elevado		Não
CQ16			Elevado		Não
CQ17	Ausência de certificação das quantidades e/ou qualidade dos bens e serviços		Elevado	Recebimento indevido de vantagem	Sim
CQ18	Apropriação/má utilização de bens públicos da instituição		Fraco	Peculato	Sim
CQ19			Fraco		Não
CQ20			Fraco		Não
CQ21			Moderado		Não
CQ22	Viciação da informação contida nas certidões		Elevado	Abuso de poder	Sim
CQ23	Favorecer/prejudicar um aluno		Elevado	Concussão	Sim

CQ24			Moderado		Não
CQ25			Moderado		Não
CQ26	Favorecimento de candidatos (procedimentos de avaliação)	Favorecimento de candidatos, através da divulgação de informação sobre os procedimentos de avaliação	Moderado	Concussão	Sim
CQ27	Favorecimento de candidatos (requisitos)	Favorecimento de candidatos, por não considerar o incumprimento de requisitos	Moderado	Peculato	Sim
CQ28			Moderado		Não
CQ29	Acesso e divulgação indevida de informação constante dos processos dos trabalhadores		Fraco	Concussão	Sim
CQ30	Alteração de documentos ou registos		Fraco	Concussão	Sim

Controlo_ID	Controlo_Nome	Controlo_Descrição	Controlo_Tipo
CONT1	Diminuição da emissão de cheques		??
CONT2	Preenchimento automático das transferências (acesso homebanking)		??
CONT3	Segregação de funções	Segregação de funções entre o registo da despesa e a emissão dos meios de pagamento	??
CONT4	Sensibilização para a boa utilização		??
CONT5	Divulgação do manual de fundo de maneio		??
CONT6	Controlo interno na plataforma informática		??
CONT7	Auditorias Internas		??
CONT8	Segregação de funções	Segregação de funções entre pedido de emissão de fatura e aprovação da mesma	??
CONT9	Conferência de valores e documento de suporte à emissão da fatura		??
CONT10	Segregação de funções	Segregação de funções entre emissão da fatura e pedido de cobrança	??
CONT11	Emissão atempada de cartas a solicitar o pagamento das faturas em atraso		??
CONT12	Verificação automática de fornecedores	Verificação automática de fornecedores por forma a evitar a possibilidade de repetição	??
CONT13	Verificação aleatória pelos Serviços de Auditoria Interna		??
CONT14	Evitação de qualquer tipo de especificação que favoreça um determinado produto/serviço	Evitação de qualquer tipo de especificação que favoreça um dado produto/serviço, designadamente no que respeita a marcas ou denominações comerciais	??

CONT15	Alternância na escolha das empresas a convidar		??
CONT16	Workflow hierarquizado de autorização dos vários procedimentos	Workflow hierarquizado de autorização dos vários procedimentos: Coordenadores de Núcleo, Coordenador da DT e CG, prévia cabimentação da despesa	??
CONT17	Utilização de cláusulas gerais de cadernos de encargos baseadas na portaria 959/2009		??
CONT18	Workflow hierarquizado de autorização dos pedidos	Workflow hierarquizado de autorização dos pedidos (Coordenadores de Núcleo, Coordenador da DT e CG) previam cabimentação da despesa	??
CONT19	Existência de documentação para justificação do não cumprimento de prazos		??
CONT20	Atos prévios de inspeção e certificação	Atos prévios de inspeção e certificação da quantidade e da qualidade dos bens e serviços	??
CONT21	Conferências físicas regulares de bens		??
CONT22	Atualização de bens abatidos e mudanças de localização		??
CONT23	Controlo interno	Controlo interno com atribuição às salas ou locais do equipamento adquirido	??
CONT24	Implementação de melhorias nas medidas de controlo de património e inventário	Implementação de melhorias nas medidas de controlo de património e inventário, já que algum equipamento não fica a ser gerido pelo GOP, mas por gestores de edifício ou outros Núcleos	??

CONT25	Necessidade de Gestão informatizada de equipamento		??
CONT26	Guardar o registo do login com o ist id do funcionário		??
CONT27	Segregação de funções	Segregação de funções: um colaborador emite o documento e, antes do mesmo ser assinado, é verificado por outro colaborador; nas certidões finais de curso o processo é verificado por três funcionários diferentes	??
CONT28	Verificação e assinatura da pauta pelo docente	A pauta é verificada e assinada pelo docente: só após a assinatura, a mesma pode ser confirmada; também fica guardado o registo do ist-id do funcionário que faz a confirmação	??
CONT29	Segregação de funções		??
CONT30	Manutenção de cópia de pagamentos realizados no processo físico do aluno	No processo físico do aluno, permanece uma cópia dos pagamentos realizados com o talão multibanco ou comprovativo de transferência bancária	??
CONT31	Procedimento concursal conduzido por um júri com um mínimo de três elementos		??
CONT32	Nomeação de júris diferenciados		??
CONT33	Atas públicas com fundamentação das decisões		??
CONT34	Apoio ao procedimento por técnicos da DRH		??
CONT35	Exigência de documentos comprovativos		??
CONT36	Homologação pelo Presidente do IST		??

CONT37	Segregação de funções	Segregação de funções: registo de alteração das situações contratuais; processamento de assiduidade; processamento de vencimentos; transferência; processamento e registo contabilístico	??
CONT38	Controlo e validação des alterações através de documento escrito		??
CONT39	Restrição de acesso aos processos e documentos		??
CONT40	Monitorização e registo de todos os acessos		??
CONT41	Acompanhamento presencial das consultas efetuadas por pessoas externas à DRH		??
CONT42	Rastreabilidade das alterações aos registos informáticos		??

Dono_ID	Dono_Nome	Dono_Descrição	*Notas dos Donos*
DONO1	Presidente		
DONO2	Vice-Presidente	Gestão Administrativa e Financeira	
DONO3	Vice-Presidente	Gestão do Campus do Taguspark	
DONO4	Vice-Presidente	Gestão do CTN	
DONO5	Vice-Presidente	Assuntos Internacionais	
DONO6	Vice-Presidente	Assuntos Académicos	
DONO7	Vice-Presidente	Assuntos de Pessoal	
DONO8	Vice-Presidente	Gestão de Instalações e Equipamentos	
DONO9	Vice-Presidente	Tecnologias de Informação e Comunicação	
DONO10	Vice-Presidente	Empreendedorismo e Ligações Empresariais	
DONO11	Vice-Presidente	Comunicação e Imagem	

DONO12	Administrador		
DONO13	Diretor de Serviços	Direção de Apoio Jurídico (DAJ)	
DONO14	Diretor de Serviços	Direção de Recursos Humanos (DRH)	
DONO15	Diretor de Serviços	Direção Técnica (DT)	
DONO16	Núcleo de Arquivo e Documentação (NAD)		Pertence à Área Comum da Direção dos Recursos Humanos
DONO17	Núcleo de Remunerações, Prestações e Benefícios Fiscais (NUR)		Pertence à Área Comum da Direção dos Recursos Humanos
DONO18	Núcleo de Prestação de Trabalho (NPT)		Pertence à Área Comum da Direção dos Recursos Humanos
DONO19	Núcleo de Docentes e Investigadores (NUDI)		Pertence à Área Especializada da Direção dos Recursos Humanos
DONO20	Núcleo de Não-docentes e Bolseiros (NNDB)		Pertence à Área Especializada da Direção dos Recursos Humanos
DONO21	Área Contabilística (AC)	Geral	Pertence à Direção Financeira
DONO22	Área Contabilística (AC)	Núcleo de Execução Orçamental (NAD)	Pertence à Direção Financeira
DONO23	Área Contabilística (AC)	Núcleo de Contabilidade (NC)	Pertence à Direção Financeira
DONO24	Área Contabilística (AC)	Núcleo de Tesouraria (NT)	Pertence à Direção Financeira
DONO25	Área Orçamental e Patrimonial (AOP)	Geral	Pertence à Direção Financeira
DONO26	Área Orçamental e Patrimonial (AOP)	Núcleo de Património (NP)	Pertence à Direção Financeira
DONO27	Área Orçamental e Patrimonial (AOP)	Núcleo de Compras e Aprovisionamento (NCA)	Pertence à Direção Financeira
DONO28	Área de Projetos (AP)	Geral	Pertence à Direção Financeira
DONO29	Área de Projetos (AP)	Núcleo de Projetos Comunitários (NPC)	Pertence à Direção Financeira

DONO30	Área de Projetos (AP)	Núcleo de Projetos Nacionais (NPN)	Pertence à Direção Financeira
DONO31	Área de Projetos (AP)	Núcleo de Projetos de Consultoria e Serviços (NPCS)	Pertence à Direção Financeira
DONO32	Área de Apoio Geral (AAG)	Geral	Pertence à Direção Técnica
DONO33	Área de Apoio Geral (AAG)	Núcleo de Serviços Gerais (NSG)	Pertence à Direção Técnica
DONO34	Área de Apoio Geral (AAG)	Núcleo de Gestão e Acompanhamento de Contratos (NGAC)	Pertence à Direção Técnica
DONO35	Área de Apoio Geral (AAG)	Núcleo de Arquivo (NArq)	Pertence à Direção Técnica
DONO36	Área de Apoio Geral (AAG)	Núcleo de Reprografia	Pertence à Direção Técnica
DONO37	Área de Apoio Geral (AAG)	Núcleo de Alojamentos	Pertence à Direção Técnica
DONO38	Área de Instalações e Equipamentos (AIE)	Geral	Pertence à Direção Técnica
DONO39	Área de Instalações e Equipamentos (AIE)	Núcleo de Obras (NO)	Pertence à Direção Técnica
DONO40	Área de Instalações e Equipamentos (AIE)	Núcleo de Manutenção (NM)	Pertence à Direção Técnica
DONO41	Área de Instalações e Equipamentos (AIE)	Núcleo de Segurança, Higiene e Saúde (NSHS)	Pertence à Direção Técnica
DONO42	Área Académica		Pertence à Direção Académica
DONO43	Núcleo de Pós-graduação e Formação Contínua		Pertence à Direção Académica
DONO44	Área Financeira		Pertence ao Taguspark
DONO45	Área Académica e de Pessoal		Pertence ao Taguspark
DONO46	Área de Serviços Administrativos		Pertence ao CTN
DONO47	Núcleo de Apoio Técnico e Logístico		Pertence ao CTN
DONO48	Todas as unidades cujos responsáveis tenham competência delegada para autorizar despesa		Não é definido/explícito no relatório
DONO49	Conselho Gestão		Não é definido/explícito no relatório

DONO50	Responsável pelo pedido de abertura do procedimento		Não é definido/explícito no relatório
DONO51	Coordenadores dos Núcleos da AT		Não é definido/explícito no relatório
DONO52	Gestores Edifícios		Não é definido/explícito no relatório
DONO53	Coordenadores do Núcleo		Dependente do núcleo a que se refere o risco
DONO54	Técnicos de Audiovisuais e Responsável		Não é definido/explícito no relatório
DONO55	Dirigentes da Direção		Não é definido/explícito no relatório
DONO56	Júris		Não é definido/explícito no relatório

B.2. Aplicação do Modelo Proposto aos Dados do LNEC

Risco					Evento	Consequência	Controlos
Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Risco_Flags	Evento_ID	Consequência_ID	Controlo_ID
R1	Existência de conflito de interesses devido a resultados de estudo solicitado condicionado por interesses de terceiros, com benefício pessoal ou privado	Moderado	RR1	RC-Gen	EV1	CQ1	CONT1; CONT2; CONT3; CONT4; CONT5; CONT6; CONT7
R2	Favorecimento de terceiros devido a desvio de estudo ou parecer para entidades terceiras, com benefício pessoal ou privado	Moderado	RR2	RC-Gen	EV2	CQ2	CONT1; CONT2; CONT3; CONT4; CONT5; CONT6; CONT7
R3		Moderado	RR3	N-Cq	EV3	CQ3	CONT1; CONT2; CONT3; CONT4; CONT5; CONT6; CONT7
R4		Moderado	RR4	N-Cq	EV4	CQ4	CONT1; CONT2; CONT3; CONT4; CONT5; CONT6; CONT7
R5		Moderado	RR5	N-Ev	EV5	CQ5	CONT1; CONT2; CONT3; CONT4; CONT5; CONT6; CONT7
R6		Moderado	RR6	RD	EV6	CQ6	CONT8; CONT9; CONT10
R7		Moderado	RR7	RD	EV7	CQ7	CONT11; CONT12; CONT13; CONT14

R8		Moderado	RR8	N-Cq	EV8	CQ8	CONT1; CONT2; CONT3; CONT5; CONT7
R9		Moderado	RR9	N-Cq	EV9	CQ9	CONT1; CONT2; CONT3; CONT5; CONT7
R10		Moderado	RR10	N-Ev	EV10	CQ10	CONT1; CONT2; CONT3; CONT5; CONT7
R11		Fraco	RR11	RD	EV11	CQ11	CONT11; CONT12; CONT13; CONT14
R12		Fraco	RR12	N-Ev	EV12	CQ12	CONT9; CONT15
R13		Moderado	RR13	N-Cq	EV13	CQ13	CONT10; CONT16; CONT17; CONT18
R14		Moderado	RR14	N-Cq	EV14	CQ14	CONT10; CONT16; CONT17; CONT18
R15		Moderado	RR15	OR	EV15	CQ15	CONT10; CONT16
R16		Elevado	RR16	N-Cq	EV16	CQ16	CONT10; CONT19
R17		Moderado	RR17	N-Cq	EV17	CQ17	CONT10
R18		Moderado	RR18	N-Ev	EV18	CQ18	CONT10; CONT16; CONT18; CONT20
R19		Moderado	RR19	N-Ev	EV19	CQ19	CONT16; CONT20
R20		Fraco	RR20	N-Ev	EV20	CQ20	CONT6
R21		Moderado	RR21	N-Ev	EV21	CQ21	CONT16; CONT21
R22		Moderado	RR22	N-Ev	EV22	CQ22	CONT22
R23		Moderado	RR23	RD	EV23	CQ23	CONT22
R24		Elevado	RR25	RD	EV24	CQ24	CONT10;CONT23
R25		Elevado	RR26	OR	EV25	CQ25	CONT10;CONT23
R26		Elevado	RR27	RD	EV26	CQ26	CONT24; CONT25; CONT26
R27		Elevado	RR28	N-Ev	EV27	CQ27	CONT24; CONT25; CONT26
R28		Elevado	RR31	N-Cq	EV28	CQ28	CONT26; CONT27
R29		Elevado	RR33	RD	EV29	CQ29	CONT28; CONT29

R30		Moderado	RR36	N-Ev	EV30	CQ30	CONT10; CONT25; CONT26
R31		Moderado	RR37	N-Ev	EV31	CQ31	CONT10; CONT25; CONT26
R32		Moderado	RR38	N-Ev	EV32	CQ32	CONT10; CONT25; CONT26
R33		Moderado	RR44	N-Ev	EV33	CQ33	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R34		Moderado	RR45	N-Cq	EV34	CQ34	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R35		Moderado	RR46	RD	EV35	CQ35	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R36		Moderado	RR47	N-Cq	EV36	CQ36	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R37		Moderado	RR48	N-Cq	EV37	CQ37	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R38		Moderado	RR49	RD	EV38	CQ38	CONT25; CONT30; CONT31; CONT32; CONT33; CONT34; CONT35
R39		Fraco	RR50	N-Ev	EV39	CQ39	CONT36; CONT37
R40		Moderado	RR51	RD	EV40	CQ40	CONT10; CONT38
R41		Moderado	RR53	N-Ev	EV41	CQ41	CONT30; CONT34; CONT35
R42		Moderado	RR54	N-Cq	EV42	CQ42	CONT30; CONT34; CONT35
R43		Moderado	RR55	RD	EV43	CQ43	CONT30; CONT34; CONT35
R44		Moderado	RR56	N-Cq	EV44	CQ44	CONT10; CONT35; CONT39; CONT40

R45		Moderado	RR61	N-Ev	EV45	CQ45	CONT41; CONT42
R46		Moderado	RR63	RD	EV46	CQ46	CONT41; CONT42
R47		Moderado	RR64	N-Cq	EV47	CQ47	CONT41; CONT42
R48	Perda, modificação ou adulteração de informação por intrusão	Moderado	RR65	RC	EV48	CQ48	CONT43; CONT44; CONT45

Evento_ID	Evento_Nome	Evento_Descrição	Likelihood	Unidade de Negócio	Atividade	Evento_Flags
EV1	Resultados de estudo solicitado condicionado por interesses de terceiros, com benefício pessoal ou privado		Fraco	C&T	Exercício ético profissional das funções	EC
EV2	Desvio de estudo ou parecer para entidades terceiras, com benefício pessoal ou privado		Fraco	C&T	Exercício ético profissional das funções	EC
EV3	Acumulação de funções incompatíveis (C&T)		Fraco	C&T	Exercício ético profissional das funções	EC
EV4	Utilização indevida dos recursos do LNEC no que concerne a instalações e equipamentos e bens (C&T)	Dependência de alguns fornecedores, nomeadamente nos casos de inexistência de um fornecedor alternativo para bens/serviços críticos para o desenvolvimento da principal atividade da empresa (por exemplo: matérias-primas, outros materiais integrados no produto, e outros materiais não integrados no produto e manutenção industrial)	Fraco	C&T	Exercício ético profissional das funções	EC
EV5			Fraco	C&T	Exercício ético profissional das funções	EC

EV6	Falha do controlo de qualidade dos procedimentos e produtos		Fraco	C&T	Controlo de qualidade	DC
EV7	Inadequação do perfil técnico e comportamental ao exercício das funções (C&T)		Fraco	C&T	Competências técnicas	DC
EV8	Utilização indevida dos recursos do LNEC no que concerne a instalações e equipamentos e bens (gestão)	Processo de aquisição incompleto (escolha fornecedor, solicitação de cotação, análise de propostas, justificação da seleção da proposta aceite, nota de encomenda, guia de remessa, receção do bem, fatura)	Fraco	Gestão (geral)	Exercício ético profissional das funções	EC
EV9	Acumulação de funções incompatíveis (gestão)	Inexistência de formalização atempada de contratos entre as partes detalhando as condições de fornecimento dos bens/serviços	Fraco	Gestão (geral)	Exercício ético profissional das funções	EC
EV10			Fraco	Gestão (geral)	Exercício ético profissional das funções	EC
EV11	Inadequação do perfil técnico e comportamental ao exercício das funções (gestão)		Fraco	Gestão (geral)	Competências técnicas	DC
EV12			Fraco	Gestão (geral)	Atendimento e relacionamento com terceiros	EC
EV13	Desvio de dinheiros e valores		Fraco	Gestão (financeira e patrimonial)	Operações contabilísticas e de Tesouraria	EC
EV14	Falhas na aplicação de normas, procedimentos e regulamentos de natureza financeira		Fraco	Gestão (financeira e patrimonial)	Operações contabilísticas e de Tesouraria	EC
EV15	Perda de valores ativos		Moderado	Gestão (financeira e patrimonial)	Gestão de recursos financeiros e patrimoniais	Outro

EV16	Pagamentos sem autorização, justificação ou confirmação da receção de bens e serviços		Moderado	Gestão (financeira e patrimonial)	Receção de bens e serviços e respetiva autorização de pagamento	EC
EV17	Transferência bancária sem base de execução		Fraco	Gestão (financeira e patrimonial)	Transferências bancárias	EC
EV18			Fraco	Gestão (financeira e patrimonial)	Produção de informação contabilística	EC
EV19			Fraco	Gestão (financeira e patrimonial)	Prestação de informação ao exterior	EC
EV20			Fraco	Gestão (financeira e patrimonial)	Apoio a outras unidades orgânicas	EC
EV21			Fraco	Gestão (financeira e patrimonial)	Apoio técnico e administrativo ao Conselho Diretivo	EC
EV22			Fraco	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	EC
EV23	Inexistência ou existência deficiente de um sistema estruturado de avaliação de necessidades	Planeamento, orçamentação e/ou estudos realizados de forma dolosa com o objetivo de tirar proveito próprio e/ou para terceiros	Fraco	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	DC
EV24	Arbitrariedade nas decisões		Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	DC
EV25	Falta de rigor orçamental		Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	Outro
EV26	Falta de nomeação diferenciada de júris para cada procedimento		Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	DC

EV27			Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	EC
EV28	Prorrogação ilegal da vigência dos contratos		Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	EC
EV29	Ausência de supervisão da execução dos contratos		Moderado	Gestão (financeira e patrimonial)	Contratação de obras, bens e serviços	DC
EV30		Cobrança de trabalhos a mais com intenção dolosa	Moderado	Gestão (financeira e patrimonial)	Procedimentos de aquisição de equipamento	EC
EV31			Moderado	Gestão (financeira e patrimonial)	Procedimentos de aquisição de equipamento	EC
EV32			Moderado	Gestão (financeira e patrimonial)	Procedimentos de aquisição de equipamento	EC
EV33			Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	EC
EV34	Intervenção no processo em situação de impedimento		Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	EC
EV35	Ausência de mecanismos que obriguem à rotatividade dos elementos integrantes dos júris		Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	DC
EV36	Utilização de critérios preferenciais pouco objetivos		Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	EC
EV37	Não disponibilização aos interessados de acesso à informação relativa ao procedimento de recrutamento e seleção		Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	EC

EV38	Ausência ou deficiente fundamentação das decisões (recrutamento e seleção de pessoal)		Fraco	Gestão (RH e logística)	Recrutamento e seleção de pessoal	DC
EV39			Fraco	Gestão (RH e logística)	Registo Individual dos Trabalhadores	EC
EV40	Falhas no registo da informação das bases de dados do pessoal		Moderado	Gestão (RH e logística)	Registo Individual dos Trabalhadores	DC
EV41			Moderado	Gestão (RH e logística)	Avaliação dos trabalhadores	EC
EV42	Utilização de critérios de avaliação pouco objetivos e/ou discricionários	Manipulação da informação de modo a facilitar o pagamento indevido de benefícios e compensações e/ou remunerações	Moderado	Gestão (RH e logística)	Avaliação dos trabalhadores	EC
EV43	Ausência ou deficiente fundamentação das decisões (avaliação dos trabalhadores)		Moderado	Gestão (RH e logística)	Avaliação dos trabalhadores	DC
EV44	Pagamentos indevidos	Manipulação deliberada na integração no processamento de salários do ficheiro com os encargos e/ou comparticipações dos Serviços Sociais respeitantes a colaboradores e familiares	Fraco	Gestão (RH e logística)	Processamento de remunerações e abonos	EC
EV45			Fraco	Gestão (RH e logística)	Controlo de assiduidade e pontualidade e do mapa de férias	EC
EV46	Justificação indevida de faltas		Fraco	Gestão (RH e logística)	Controlo de assiduidade e pontualidade e do mapa de férias	DC
EV47	Atribuição de dias de férias em número superior ao que o trabalhador tem direito		Fraco	Gestão (RH e logística)	Controlo de assiduidade e pontualidade e do mapa de férias	EC

EV48	Intrusão		Fraco	Gestão (sistemas de informação)	Manutenção e suporte	EC

Consequência_ID	Consequência_Nome	Consequência_Descrição	Impacto	Consequência_Tipo	ConqEstruturada_Flags
CQ1	Existência de conflito de interesses	Existência de conflito de interesses via condicionamento de estudo	Elevado	Tráfico de influência	Sim
CQ2	Favorecimento de terceiros	Favorecimento de terceiros via divulgação de estudo ou parecer	Elevado	Tráfico de influência; violação de segredo por funcionário	Sim
CQ3			Elevado		Não
CQ4			Elevado		Não
CQ5	Quebra da reserva da confidencialidade (C&T)		Elevado	Violação de segredo por funcionário	Sim
CQ6			Elevado		Não
CQ7			Elevado		Não
CQ8			Elevado		Não
CQ9			Elevado		Não
CQ10	Quebra da reserva da confidencialidade (gestão)		Elevado	Violação de segredo por funcionário	Sim
CQ11			Moderado		Não
CQ12	Prestação de informação inadequada		Moderado	Concussão	Sim
CQ13			Elevado		Não
CQ14			Elevado		Não
CQ15			Moderado		Não
CQ16			Elevado		Não
CQ17			Elevado		Não

CQ18	Afetação da qualidade da prestação de contas e da informação contabilística		Elevado	Concussão	Sim
CQ19	Deficiente qualidade da informação financeira prestada a entidades externas		Elevado	Concussão	Sim
CQ20	Perda de qualidade da informação prestada e do apoio técnico e administrativo às unidades orgânicas		Moderado	Concussão	Sim
CQ21	Redução da qualidade da informação prestada e do apoio técnico e administrativo para a tomada de decisão do CD		Elevado	Concussão	Sim
CQ22	Violação de disposições legais e principios gerais de contratação pública		Elevado		Não
CQ23			Elevado		Não
CQ24			Elevado		Não
CQ25			Elevado		Não
CQ26			Elevado		Não
CQ27	Conflito de interesses dos elementos do júri		Elevado		Não
CQ28			Elevado		Não
CQ29			Elevado		Não
CQ30	Avaliação incorreta no contexto que justifica a aquisição		Moderado	Concussão	Sim
CQ31	Favorecimento de fornecedor		Moderado	Tráfico de influência	Sim

CQ32	Existência de conflito de interesses		Moderado	Tráfico de influência	Sim
CQ33	Discricionariedade ou favorecimento de candidatos		Elevado	Tráfico de influência	Sim
CQ34			Elevado		Não
CQ35			Elevado		Não
CQ36			Elevado		Não
CQ37			Elevado		Não
CQ38			Elevado		Não
CQ39	Acesso indevido às informações		Moderado	Peculato; violação de segredo por funcionário	Sim
CQ40			Moderado		Não
CQ41	Discricionariedade ou favorecimento na avaliação de trabalhadores		Moderado	Tráfico de influência	Sim
CQ42			Moderado		Não
CQ43			Moderado		Não
CQ44			Elevado		Não
CQ45	Discricionariedade ou favorecimento (controlo de assiduidade e pontualidade e do mapa de férias)		Elevado	Tráfico de influência	Sim
CQ46			Elevado		Não
CQ47			Elevado		Não
CQ48	Perda, modificação ou adulteração de informação		Elevado	Concussão	Sim

Controlo_ID	Controlo_Nome
CONT1	Acompanhamento e supervisão pelos dirigentes do rigoroso cumprimento dos princípios e normas éticas inerentes às funções
CONT2	Observância de orientações e mecanismos que garantam a prevenção e o cumprimento dos princípios e valores éticos
CONT3	Observância de medidas conducentes a prevenir a quebra de sigilo, designadamente quanto aos mecanismos de acesso e acompanhamento restrito dos processos, nas suas diferentes fases
CONT4	Preferência da colegialidade na realização das acções, com especial relevância nas de controlo
CONT5	Declaração ética sobre conflito de interesses e impedimentos
CONT6	Acompanhamento e supervisão em todos os procedimentos e operações
CONT7	Rotatividade adequada do pessoal
CONT8	Supervisão e revisão dos procedimentos adoptados e dos produtos elaborados
CONT9	Adopção e difusão das melhores práticas e conhecimentos
CONT10	Segregação de funções
CONT11	Mecanismos de aferição dos comportamentos no exercício das funções
CONT12	Adequação das necessidades formativas ao perfil exigido
CONT13	Motivação individual e dos grupos de trabalho
CONT14	Partilha de conhecimentos, experiências e informação técnica
CONT15	Definição de níveis de responsabilidade

CONT16	Conferências da informação intermédia e final
CONT17	Acompanhamento e controlo da execução das medidas previstas na norma de controlo interno
CONT18	Responsabilidade das operações
CONT19	Processo formal de autorização dos processos aquisitivos e da autorização da despesa e procedimento para validação das faturas ou documentos equivalentes
CONT20	Medidas para controlo de prazos
CONT21	Análise e revisão permanente da execução dos procedimentos legais e dos estabelecidos no sistema de controlo interno
CONT22	Implementação de um sistema estruturado de avaliação das necessidades
CONT23	Controlo da tramitação dos processos de acordo com as prioridades estabelecidas
CONT24	Nomeação diferenciada de júris para cada procedimento
CONT25	Declaração de inexistência de conflito de interesses
CONT26	Controlo interno através de auditoria
CONT27	Gestão da carteira de contratos
CONT28	Reforço do controlo interno na fase de execução dos contratos
CONT29	Relatórios de progresso
CONT30	Utilização de critérios objetivos e precisos, com reduzida margem de discricionariedade
CONT31	Nomeação de júris diferenciados para os concursos
CONT32	Rotatividade dos elementos dos júris dos concursos
CONT33	Permissão e facilitação do acesso à informação sobre o procedimento concursal

CONT34	Fundamentação das decisões
CONT35	Cumprimento da legislação aplicável
CONT36	Medidas de segurança nos arquivos dos processos individuais
CONT37	Acesso restrito aos funcionários da Secção de Pessoal e interessados
CONT38	Cruzamento de informação e realização de testes
CONT39	Verificação das folhas de abonos e descontos mensais
CONT40	Manual de procedimentos
CONT41	Publicitação e cumprimento do regulamento de horário de trabalho
CONT42	Existência de sistema informático de gestão da assiduidade
CONT43	Procedimentos de controlo de acessos, autorização e autenticação dos recursos e serviços de Tecnologias de Informação disponibilizados
CONT44	Procedimentos de classificação da informação em termos de confidencialidade e de partilha pelos utilizadores
CONT45	Aplicação de medidas de segurança aos pontos de controlo da rede e regulação do tráfego de dados