



Gestão do Risco Empresarial, incluindo os Riscos de Corrupção e Infrações Conexas

Versão	Data	Descrição
00	19/08/2011	Criação do documento
01	25/02/2015	Revisão decorrente da fusão APDL APVC
02	16/07/2015	Identificação e autonomização dos riscos de corrupção e infrações conexas, respetivas medidas de prevenção e controlo e das oportunidades de melhorias - Anexos I, II e III

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Sumário

1.	Introdução à gestão de risco.....	3
1.1	Gestão de risco empresarial.....	3
2.	Objetivos.....	6
2.1	Auditoria Interna e Gestão de Risco	6
2.2	Objetivos da Gestão de Risco	6
3.	Processo de Gestão de risco	7
3.1	Fase 1 – Estabelecer contexto	7
3.2	Fase 2 – Identificar riscos.....	20
3.3	Fase 3 – Analisar riscos	21
3.4	Fase 4 – Avaliar riscos	26
3.5	Fase 5 – Tratar riscos.....	28
3.6	Comunicação e consulta	30
3.7	Monitorização e revisão.....	33
4.	Critérios para gestão de risco	34
4.1	Funções e responsabilidades	34
4.2	Organização dos riscos	35
4.3	Critérios de probabilidade e de impacto dos riscos	40
4.4	Classificação do nível de controlo.....	42
4.5	Níveis de aceitação de risco.....	43
4.6	Indicadores de alerta de risco.....	44
4.7	Estratégias para tratamento de risco	45
4.8	Identificação de interlocutores e “donos” dos riscos	46

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

1. Introdução à gestão de risco

1.1 Gestão de risco empresarial

Desde a publicação e entrada em vigor do DL 211/2008, de 3 de novembro, que criou a sociedade anónima de capitais exclusivamente públicos designada então por APVC – Administração do Porto de Viana do Castelo, S.A., integralmente subscrito e realizado pela APDL – Administração dos Portos do Douro e Leixões, S.A., que estas entidades partilhavam o mesmo Conselho de Administração, por imposição estatutária da primeira.

Com efeito, desde então, existia na estrutura organizativa a preocupação e algumas práticas, ainda que pontuais, na partilha de competências técnicas entre as várias áreas corporativas das duas unidades empresariais.


Inclusive, dando seguimento a uma recomendação do Tribunal de Contas – para que fossem implementados procedimentos que permitissem à APVC beneficiar, de modo mais amplo, das competências técnicas da APDL - foram estudados mecanismos de racionalização de recursos, exploração de sinergias e de economias de complementaridade e bem assim a aplicação de algumas práticas que potenciasssem a referida partilha de Competências/Serviços (conforme deliberado na sessão do Conselho de Administração nº 42/2013).

Mais recentemente, no segundo semestre de 2014, o até aí modelo de gestão de entidades juridicamente autónomas, em que a APDL detinha uma participação dominante nos capitais da entidade participada (APVC), evoluiu para um processo de fusão entre estas empresas, ao que designou por Projeto Aliança APDL | APVC.

Este projeto é formalmente concretizado a 8 de janeiro de 2015 por registo definitivo na Conservatória do Registo Comercial, com efeitos a 01 de janeiro do mesmo ano, tendo daí resultado uma só entidade jurídica, com a designação de APDL – Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A., doravante abreviadamente designada por APDL.

Do exposto resulta, ter sido premente, a extensão às estruturas do porto de Viana do Castelo da gestão do risco empresarial incluindo os riscos de corrupção e infrações conexas (internamente conhecido por **projeto MAR**), vigente na APDL desde 2011, objetivada, entre outros documentos, no presente Manual.

Atentos às permanentes mudanças nas formas de funcionamento das empresas e negócios, o aumento da consciência ambiental na sua articulação com o desenvolvimento sustentável e o progressivo acréscimo de responsabilidade das empresas e dos membros dos seus órgãos de gestão, vêm confirmando as insuficiências dos tradicionais princípios de gestão empresarial. Assim sendo, os gestores estão cada vez mais conscientes da necessidade de terem ao seu dispor meios

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

que os ajudem no processo de tomada de decisões, constituindo a gestão de risco, um dos elementos mais relevantes nos modernos princípios de gestão empresarial.

Muito embora noutros países, designadamente nos EUA, a gestão de risco tenha vindo a ser objecto de estudo e de aplicação prática desde a segunda metade do século passado, só mais recentemente é que a informação dos riscos do negócio e o seu controlo têm vindo a constituir, com maior abrangência, um tema nuclear nos modernos princípios de gestão empresarial.

A gestão de risco trata pois de uma abordagem completa e sistemática que visa ajudar as organizações, independentemente da sua dimensão ou missão, a identificar eventos e a medir, priorizar e responder aos desafios de risco dos projetos e iniciativas que assumem. Esta abordagem permite às organizações determinar o nível de risco que podem, ou querem aceitar, na procura de criar valor para os seus investidores. A existência de incertezas pode provocar situações de risco como de oportunidades, as quais tanto podem retirar como acrescer valor, oferecendo esta abordagem uma estrutura para gerir eficazmente a incerteza, respondendo aos riscos e explorando as oportunidades que surjam.


Atualmente a gestão de risco é um processo chave em qualquer organização. O seu desenho e implementação são influenciados pelas variadas necessidades das organizações, pelos seus objetivos particulares, as suas unidades de negócio, os seus processos e pelas práticas desenvolvidas, optando-se, face à similitude no funcionamento das estruturas integrantes dos portos do Douro, Leixões e de Viana do Castelo, por uma única metodologia.

Reflexo da importância que a gestão de risco tem vindo a assumir no contexto das organizações é a publicação da norma ISO 31000 “Gestão de risco”, consubstanciada em três documentos que visam auxiliar as organizações na adoção de um modelo de gestão de risco.

De acordo com esta norma, a gestão de risco numa organização deverá:

- a) Criar valor;
- b) Ser parte integrante dos processos da organização;
- c) Fazer parte do processo de tomada de decisão;
- d) Endereçar explicitamente a incerteza;
- e) Ser sistemática, estruturada e atempada;
- f) Basear-se na melhor informação disponível;
- g) Adaptada à organização;
- h) Ter em consideração factores humanos e culturais da organização;
- i) Ser transparente e abrangente;
- j) Ser dinâmica, interactiva e com capacidade de resposta à mudança; e
- k) Ser um elemento facilitador da melhoria contínua e valorização da organização.

No domínio específico dos portos, e mais concretamente das autoridades portuárias, as principais orientações para gestão dos riscos focam-se essencialmente nas operações portuárias, em particular nas questões de segurança intrínseca e extrínseca (“*safety*” e “*security*”) e de proteção ambiental.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

É igualmente relevante o peso que as recomendações emitidas por organismos oficiais têm vindo a assumir recentemente no sentido da adopção e reforço dos sistemas de gestão de risco, tanto a nível corporativo^{1, 2, 3 e 4} como a nível operacional⁵.

Este documento consubstancia a resposta integrada da Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A., doravante abreviadamente designada por “APDL”, aos desafios da gestão de risco, cujos principais benefícios se podem agregar em três vértices.

Em primeiro lugar, a gestão de risco representa para a APDL um instrumento essencial para a tomada de decisão através da permanente monitorização dos riscos a que a Empresa se encontra exposta, sensibilizando a organização de uma forma abrangente, para uma cultura de risco que inclua a perspectiva de evitar riscos mas também a perspectiva positiva de assumir riscos.

Por outro lado, as Direções beneficiam da gestão de risco através da possibilidade de antecipar situações de incerteza, mitigando os riscos de consequências adversas e potenciando os riscos que encerram em si oportunidades. É ainda obtida uma maior e mais sustentada capacidade de decisão da organização face a eventos de risco, respondendo de forma coordenada e integrada a riscos com causas, impactos ou vulnerabilidades que abranjam mais do que uma Direção.

Por último, do ponto de vista da Auditoria Interna e do ambiente de controlo, a gestão de risco assume uma especial relevância, através da possibilidade de avaliação contínua do perfil de risco da organização e do reforço do nível de controlo interno na organização. É igualmente relevante a contribuição da gestão de risco para a Auditoria Interna, orientando a sua ação para as áreas / processos de maior risco e preocupação para o negócio – “Auditoria Interna baseada no Risco”.

Como resultado imediato desta abordagem, será possível planear e executar periodicamente ações de auditoria que tenham em consideração os riscos mais relevantes para a organização, através de uma metodologia para planeamento de auditorias.


¹ “O órgão de administração deve criar e manter um sistema de controlo adequado à dimensão e à complexidade da empresa, em ordem a proteger os investimentos da empresa e os seus activos. Tal sistema deve abarcar todos os riscos relevantes assumidos pela empresa”. *RESOLUÇÃO DO CONSELHO DE MINISTROS nº 49/2007 – Estatuto do Gestor Público / Princípios de bom governo das empresas do sector empresarial do Estado, nº 19*

² “Compete ao fiscal único ou conselho fiscal (...) fiscalizar a eficácia do sistema de gestão de riscos, do sistema de controlo interno e do sistema de auditoria interna, se existentes”. *CÓDIGO DAS SOCIEDADES COMERCIAIS Art. 420º, nº1, al. i)*

³ “As sociedades devem criar sistemas internos de controlo, para a deteção eficaz de riscos ligados à actividade da empresa, em salvaguarda do seu património e em benefício da transparência do seu governo societário”. *CMVM Recomendação N.º 7/2007– Código de Governo das Sociedades, II. 1.1.2*

⁴ “Compete à comissão de auditoria (...) Avaliar os sistemas de controlo interno e de risco”. Decreto-Lei n.º 558/99, de 17 de Dezembro alterado pelo Decreto-Lei n.º 300/2007, de 23 de Agosto – *Regime jurídico do sector empresarial do Estado, Art. 18º-E, nº1, al. f)*

⁵ Código ISPS – DIRECTIVA 2005/65/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 26 de Outubro de 2005 relativa ao reforço da segurança nos portos, transposta para a legislação nacional através do Decreto-Lei n.º 226/2006, de 15 de Novembro.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

2. Objetivos

O objetivo deste documento consiste em dotar a APDL de um manual para o processo de gestão de risco empresarial que permita identificar, avaliar, tratar e monitorizar todos os seus principais riscos a nível empresarial, de uma forma eficiente e adequada. Para alcançar este desiderato foi seguida a recente norma ISO 31000 e o *standard* "COSO II - *Integrated framework for Enterprise Risk Management*" (adiante designado apenas por "COSO II").

2.1 Auditoria Interna e Gestão de Risco


A atividade da Auditoria Interna beneficia assim, da existência de um sistema de gestão de riscos empresariais no Porto de Viana do Castelo, uma vez que poderá orientar as suas ações de auditoria para as áreas mais expostas ao risco e no acompanhamento das oportunidades de melhoria concebidas no âmbito deste projeto, do Modelo de Avaliação de Riscos.

Como veremos mais à frente, alguns riscos estão sobretudo relacionados com os processos da organização e as suas infra-estruturas. Uma vez que o âmbito de atuação da Auditoria Interna é fundamentalmente ao nível dos processos de negócio, a sua ação irá centrar-se essencialmente nesta categoria de riscos.

2.2 Objetivos da Gestão de Risco

A gestão do risco empresarial agora endereçada irá melhorar a capacidade de gestão face à ocorrência de eventos de risco, através da permanente monitorização dos riscos existentes:

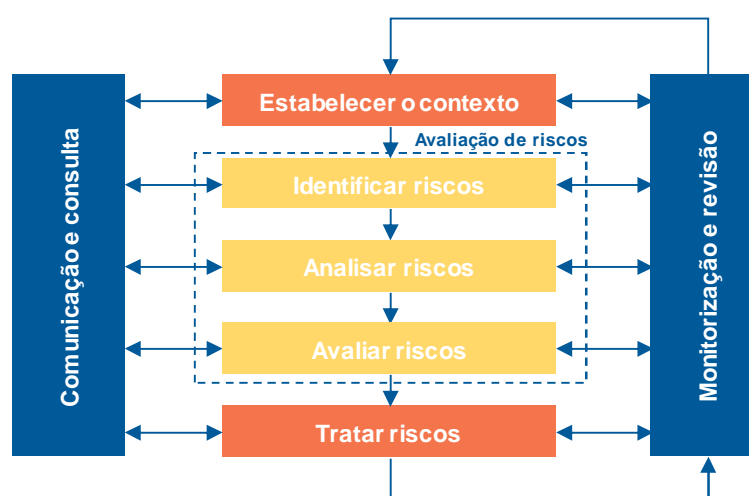
- Definir e implementar um Modelo de Gestão de Riscos que permita a identificação, categorização e priorização dos principais riscos (ameaças / oportunidades) que possam afetar a prossecução dos objetivos de negócio da APDL;
- Dotar a APDL dos meios, ferramentas, mecanismos e rotinas para gestão dos riscos identificados; e
- Promover a aproximação do trabalho de Auditoria Interna às preocupações das várias direções da APDL e dos seus *stakeholders*.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

3. Processo de Gestão de risco

O processo de gestão de risco da APDL segue as melhores práticas, modelos e *frameworks* de gestão de risco internacionalmente aceites, entre os quais se encontram o “COSO II - *Integrated framework for Enterprise Risk Management*”, o “*Risk Management Standard AS/NZS 4360 : 2004*” e mais recentemente a norma ISO 31000.

Para a elaboração do processo de gestão de risco foi seguida a norma ISO 31000 no que concerne às principais fases do mesmo, e o COSO II para a sistematização e estruturação dos riscos. Este processo é composto por um conjunto de sete fases inter-relacionadas, englobando em si mesmo um processo iterativo de melhoria contínua, consubstanciado por um processo de comunicação e consulta e por um processo de monitorização e revisão. A figura abaixo representa esquematicamente o fluxo do processo de gestão de risco.




Nos capítulos seguintes serão descritas com maior detalhe cada uma das fases representadas acima.

3.1 Fase 1 – Estabelecer contexto

Esta fase tem como objetivo a definição do âmbito da gestão de risco nomeadamente em relação a:

Elaborado: AIQ Data: 14/07/2015	Aprovado: CA Data: 16/07/2015	Página 7 de 47
------------------------------------	----------------------------------	----------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015


- Identificação do contexto externo à organização;
- Identificação do contexto interno à organização;
- Identificação do âmbito organizacional da gestão de risco; e
- Definição de um conjunto de critérios através dos quais os riscos irão ser avaliados.

Contexto Externo

A definição do contexto externo é um dos aspetos a ter em consideração quando se efetua a análise de risco de uma organização. Aspetos culturais, sociais, políticos, competitivos, sobretudo a nível internacional influenciam no alcançar dos objetivos definidos para a organização.

No âmbito da evolução e das principais tendências no setor dos transportes marítimos, são de destacar alguns desafios com que este setor se depara:

- **Globalização** – Este efeito sentido nos mais variados setores, apresenta-se no setor do transporte marítimo como um dos que mais influencia a sua evolução. A globalização fez aumentar o volume de mercadorias transportadas mas também a forma de a transportar. É consequência directa o sistema radial (“hub-and-spoke”) de transporte de mercadorias, onde o papel de cada porto terá que ser visto no contexto global e não numa perspetiva somente nacional;
- **Liberalização e privatização** – Assistimos a uma tendência para os governos atuarem como agentes de regulação e de autoridade em vez de serem operadores dos portos. Por outro lado, é de esperar uma concentração de operadores a nível mundial que procuram obter economias de escala. Num contexto de economia global, a competitividade dos portos será afetada por estes dois movimentos;
- **Crescimento da dimensão dos navios** – A tendência para navios maiores, conduz a uma consolidação do tráfego dos navios em relativamente poucos portos – os de maior dimensão – sendo o impacto nos restantes portos dependente da distribuição do transporte entre transporte rodoviário e transporte marítimo costeiro. Neste aspeto é relevante a capacidade dos portos, não só ao nível das infra-estruturas para acomodar navios de maiores dimensões (comprimento e calado), como também na eficiência das operações que permita responder aos requisitos bastante mais exigentes com este tipo de navios (e.g. escalas programadas com maior antecedência e por isso menos flexíveis, necessidade de menores tempos de escala);
- **Aumento da contentorização das mercadorias** – Esta tendência é reflexo de um movimento ascendente na cadeia de valor ao nível das exportações (e.g. exportação de produtos acabados em vez de matérias primas). Neste aspecto é importante a capacidade dos portos na movimentação de mercadorias contentorizadas, face a outras alternativas;
- **Integração com outros meios de transporte** – A dimensão do *hinterland* dos portos e a sua integração com outros meios de transporte com capacidade para dar resposta ao volume de mercadorias movimentado é fundamental para a eficiência operacional dos portos. Esta

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

integração e capacidade intermodal assume particular relevância num contexto de crescimento dos navios devido à necessidade de maiores requisitos logísticos (armazenagem temporária); e

- **Segurança e ambiente** – Em consequência da maior tensão política e dos atos terroristas ocorridos no passado, foi introduzida uma nova regulamentação de segurança em meados da década passada (código ISPS – *International Ship and Port Facility Security*). Este código obrigou os portos a adotarem medidas mais restritivas ao nível da segurança que se refletem na atividade diária dos mesmos. Do ponto de vista ambiental, o impacto da atividade portuária nas comunidades locais é grande, existindo uma forte pressão exercida por estas comunidades para um reforço das medidas ambientais. Por outro lado, são encorajados os esforços no sentido de reduzir a pegada ecológica dos portos, por exemplo através da geração e utilização de energias renováveis.

Contexto interno

É indiscutível a relevância que o mar e todas as atividades que lhe estão associadas representam para o país. Esta importância manifesta-se em orientações estratégicas delineadas pelo estado nos últimos 10 a 15 anos. São de particular relevância, de entre os vários documentos que abordam este tema, o livro branco “Política Marítimo-Portuária Rumo ao Século XXI” apresentado em 1997, o livro verde “Uma visão europeia para os oceanos e os mares” de 2006 e as “Orientações estratégicas para o setor marítimo portuário”, também apresentadas em 2006.

O modelo orgânico da APDL enquanto autoridade portuária, resultante das alterações introduzidas pelo Decreto-Lei 335/98, de 3 de Novembro, permitem contextualizar a sua atividade e os principais *stakeholders*, os dois aspectos mais relevantes quando pretendemos caracterizar o contexto interno da organização.


O aumento do *hinterland* das estruturas portuárias adstritas à APDL, com a recente fusão do porto de Viana do Castelo, a 01 de janeiro de 2015.

A evolução dos quadros legais e regulamentares e a crise económica e financeira mundial traduzem, ou induzem necessariamente na evolução dos sistemas de governação das organizações e no reforço das competências e dos meios de sistemas de gestão de riscos e de controlo, constituindo prioridades dos dirigentes das entidades.

Atinente a essa realidade, desde há algum tempo que a APDL tem vindo a definir e implementar interna e externamente na Comunidade Portuária, diversas medidas que se querem fomentadas (verdadeiros contributos) de uma ideologia organizacional no sentido da dissuasão da corrupção e da fraude, em abono de uma gestão transparente, do crescimento sustentável e integrado, de comportamentos adequados e credíveis aos olhos dos *Stakeholders*, nomeadamente, com a definição e implementação, desde 2011, do Modelo de Avaliação de Riscos Empresarial.

Volvidos três anos da implementação do projeto MAR – Modelo de Avaliação dos Riscos no portos do Douro e Leixões e aproveitando as recomendações nesta temática, era premente o ajustamento deste modelo à emergente estrutura orgânica, pós fusão.

Importa aqui sintetizar as alterações institucionais mais significativas verificadas nos últimos anos.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O projeto governamental de reformulação dos instrumentos e modelos de gestão do sector portuário nacional determinaram a transformação jurídica da APDL, de Instituto Público passou a Sociedade Anónima em Dezembro/1998 com competências e responsabilidades de cariz fortemente empresarial,

Com vista a criar as condições para essa alteração jurídico-institucional, a política de recursos humanos da empresa nos anos que a antecederam, foi caracterizada pelo incentivo às aposentações antecipadas, visando também privilegiar a estabilização do quadro de pessoal, designadamente nas áreas operacionais, reduzindo significativamente o quadro de efetivos,

Paralelamente, foi integrado na estrutura hierárquico-funcional da organização o Departamento de Pilotagem que dependia de diferente ministério, refletindo-se numa melhor articulação desses meios humanos e operacionais.

Em 2009, a necessidade de se garantir a continuidade da assistência médica e de saúde, até aqui exclusivamente assegurada pela empresa, foi decidido a passagem para a ADSE de todos os colaboradores com vínculo às Obras Sociais (sistema de saúde próprio), mantendo-se este como um sistema complementar.


Já mais recentemente, com efeitos a 01 de janeiro de 2015, concretizou-se a fusão do Porto de Viana do Castelo aos Portos do Douro e Leixões, passando a nova empresa a designar-se por APDL – Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A..

Atualmente, a APDL é uma Sociedade Anónima de capitais exclusivamente públicos, que tem por objeto a administração dos portos do Douro, Leixões e Viana do Castelo, visando a sua exploração económica, conservação e desenvolvimento abrangendo o exercício das competências e prerrogativas de autoridade portuária que lhe estejam ou venham a estar cometidas.

A sua área de jurisdição abrange cinco zonas, a saber:

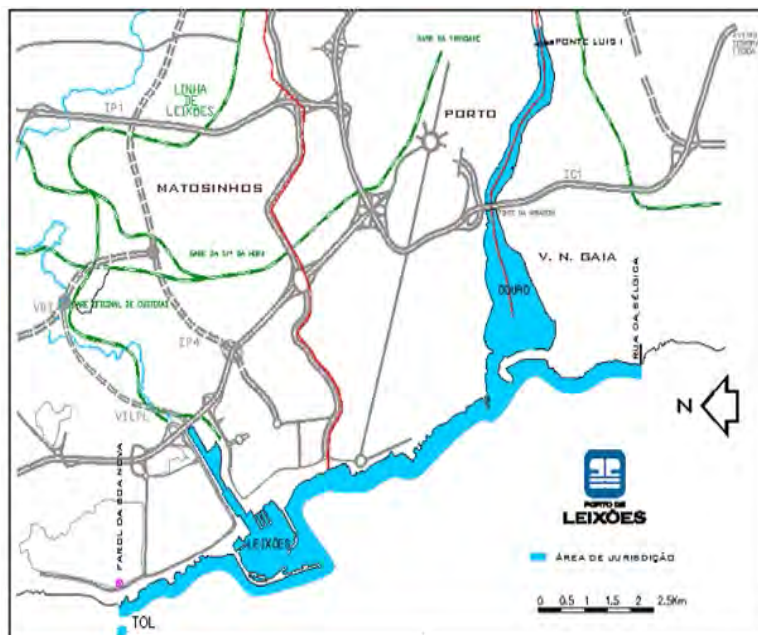
- **Faixa marginal do domínio público marítimo**, desde o enfiamento do eixo da Rua da Bélgica, na Praia de Lavadores, até ao paralelo do farol da Boa Nova, a norte do Porto de Leixões.
- **Porto do Douro**, que inclui todo o estuário do Rio Douro, desde 200 metros a montante da Ponte Luís I até à foz, com todas as suas margens, ancoradouros, cais, docas e terraplenos existentes ou que venham a ser construídos;
- **Zona do Porto de Leixões**, que abrange quebra-mares, a área molhada por eles circunscrita e as docas existentes ou a construir; o curso do Rio Leça até à antiga ponte dos moinhos de Guifões e a área terrestre delimitada pelo domínio público respetivo.
- **Terminal Oceânico de Leixões (TOL)**, localizado a cerca de 3 milhas a oeste do farol da Boa Nova.

Zona do Porto de Viana do Castelo, na margem norte inicia-se na doca de recreio de montante junto ao parque da cidade, prolongando-se até ao espelho de água adjacente à marina, seguindo junto à marginal até à antiga doca comercial, que fica incluída, juntamente com os armazéns da doca de marés, continuando pelo limite exterior dos estaleiros navais, até ao parque empresarial da praia norte, seguindo para a avenida do atlântico até ao

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015


enraizamento do molhe norte, continuando depois para sul pelo alinhamento deste molhe até ao farol. Na margem sul, inicia-se na ponte Eiffel, seguindo junto à estrada nacional 13-5 (Avenida do Cabedelo) até à praia do cabedelo, a cerca de 50 metros a sul do molhe sul.

Portos do Douro e Leixões



Porto de Viana do Castelo



	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015


Na infraestrutura portuária da APDL, uma das maiores de Portugal e a maior do Noroeste Peninsular, movimenta-se todo o tipo de cargas e destaca-se pelos elevados índices de competitividade e eficiência que apresenta.

Por esta passa cerca de 1/4 do comércio externo português, movimentando todo o tipo de cargas, num total de mais de 18,1 milhões de toneladas/ano, recebendo cerca de 2.609 navios/ano e obteve o seu record mensal em Abril/2013, com 1,73 milhões de toneladas.

Entre a oferta de serviços prestados pela APDL contam-se:

- Ajudas à Navegação;
- Gestão de postos de acostagem;
- Controle de tráfego marítimo;
- Prestação de serviços de amarração, armazenagem, aguada, recolha de resíduos, fornecimento de energia eléctrica, reboque e pilotagem;
- Manutenção dos Canais de Acesso;
- Prevenção e combate à poluição no mar;
- Sistemas de Segurança;
- Construção e manutenção de acessibilidades terrestres ao porto;
- Manutenção de equipamentos, cais e terraplenos;
- Limpeza da área portuária;
- Brokerage de informação na Comunidade Portuária e entre esta e os organismos da Administração Central do Estado, através da JUP;
- Publicação de Serviços UDDI (Universal Description Discovery and Integration) para utilização pelos Sistemas Logísticos, no âmbito das Auto-Estradas do Mar;
- Publicação de medidas de desempenho, personalizadas ou agregadas, e informação de gestão do porto.

Tendo em vista a manutenção de um serviço de interesse público, disponibiliza e assegura as seguintes infra-estruturas portuárias:

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Em Leixões,




- (1) Estação de Passageiros
- (2) Terminal Roll-On / Roll-Off
- (3) Instalações Especializadas (silos, depósitos e armazéns)
- (4 e 10) Cais de movimentação de Granéis Líquidos
- (5) Terminal de Petroleiros
- (6) Terminal de Contentores
- (7) Cais Convencionais de Carga Geral e Granéis Sólidos
- (8) Doca de Recreio
- (9) Porto de Pesca

Em Viana do Castelo:



- (1) Porto Comercial
- (2) Enercon / Estaleiros Navais de Viana do Castelo
- (3) Doca de Recreio a Jusante da Ponte Rodo-Ferroviária
- (4) Doca de Recreio a Montante da Ponte Rodo-Ferroviária
- (5) Futura Marina Oceânica (Reconversão da Antiga Doca Comercial)
- (6) Porto de Pesca
- (7) Docapesca
- (8) Pilotos

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O modelo de gestão empresarial adotado no final de 1998, baseado numa alteração do objeto comercial até aí com uma forte intervenção enquanto prestador de serviços, sofreu profundas alterações passando a APDL, essencialmente, a ser o garante e controlador do cumprimento das condições contratualmente fixadas a agentes económicos do sector privado a quem eram ou passariam a ser atribuídas as concessões às áreas de exploração portuária.

Deste modo, para a prossecução desse desiderato, a APDL conta com a atuação de um conjunto de *players*, de natureza institucional e de empresas particulares, dos quais se destacam:

IPTM – Instituto Portuário e dos Transportes Marítimos

Tem por missão regular, fiscalizar e exercer funções de coordenação e planeamento do setor marítimo-portuário e supervisionar e regulamentar as atividades desenvolvidas neste setor.

No porto de Leixões, o IPTM tem uma delegação – *Port State Control* que realiza inspeções aos navios relativas à segurança de navegação, segurança da vida humana no mar, cumprimento de Convenções Internacionais, entre outros aspetos.

Alfândegas de Leixões e de Viana do Castelo

A Alfândega é um serviço periférico da Autoridade Tributária e Aduaneira (AT).

A AT é um serviço da administração direta do Estado dotado de autonomia administrativa, dispendo de unidades orgânicas desconcentradas de âmbito regional, designadas por direções de finanças e alfândegas, e de âmbito local, designadas por serviços de finanças, delegações e postos aduaneiros.


Tem por missão administrar os impostos, direitos aduaneiros e demais tributos que lhe sejam atribuídos, bem como exercer o controlo da fronteira externa da União Europeia e do território aduaneiro nacional, para fins fiscais, económicos e de proteção da sociedade, de acordo com as políticas definidas pelo Governo e o Direito da União Europeia.

Assim sendo, as Alfândegas são responsáveis quer pela proteção da Sociedade quer pela facilitação do comércio internacional, através da gestão da fronteira externa e da garantia de segurança da cadeia logística.

Capitanias de Leixões e de Viana do Castelo (Autoridades Marítimas)

A Direção-Geral da Autoridade Marítima – DGAM – é o serviço responsável pela direção, coordenação e controlo das atividades exercidas no âmbito da Autoridade Marítima Nacional (AMN).

A Autoridade Marítima presta serviços às tripulações, às cargas e aos navios, nomeadamente vigilância, policiamento, controlo e fiscalização do cumprimento dos normativos legais aplicáveis na área do porto, visita e desembarço do navio, entre outros serviços administrativos e técnicos.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

As Capitánias dos Portos (CP), como órgãos locais da DGAM, constituem o núcleo orgânico fundamental de toda a AMN, quer pelo quadro de competências que a lei lhe concede, algumas em exclusividade, quer pela proximidade com as comunidades ribeirinhas, que servem localmente em razão da respetiva jurisdição territorial e, consequentemente, ao formato de descentralização pelo qual se encontram dispersas por todo o território nacional.

As Capitánias dos Portos são repartições marítimas abertas ao público, servindo especialmente as comunidades piscatórias, da navegação de comércio, de recreio e marítimo-turística, competindo-lhes a prática de atos administrativos específicos deste tipo de utentes (emissão de licenças e de certidões, registo de embarcações, vistos em documentos, etc.).

TCL – Terminal de Contentores de Leixões, S.A. (6)

Esta empresa desenvolve a actividade de movimentação de cargas contentorizadas desde Maio de 2000 – por um período de 25 anos, eventualmente prorrogável por mais 5 anos –, em regime de concessão do serviço público, compreendendo:


- os serviços de movimentação de contentores de e para os navios atracados nos cais do terminal;
- as operações de tráfego, estacionamento, recepção e expedição de contentores;
- as operações respeitantes a mercadorias transportadas em contentores (armazenagem, conferência, assistência a contentores frigoríficos e outras);
- as diligências necessárias ao seu desembarço junto das entidades competentes (estatuto de depositário e de armazém de exportação);
- as operações respeitantes a carga não contentorizada que constitua complemento da carga dos navios acostados no terminal;
- o serviço de limpeza, manutenção e reparação de contentores.

TCGL – Terminal de Carga Geral e Granéis de Leixões, S.A. (7)

Os cais para a movimentação de carga geral fraccionada e de granéis sólidos encontram-se concessionados a esta empresa desde Julho de 2001 - por um período de 25 anos, eventualmente prorrogável por mais 5 anos.

Repartem-se entre os cais convencionais do lado Norte e do lado Sul e respectivos terraplenos adjacentes.

Os serviços prestados no âmbito desta concessão compreendem:

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- os serviços de movimentação da carga geral fraccionada e granéis de e para os navios atracados nos cais convencionais, incluindo as operações de recepção e estiva ao embarque e as operações de desestiva e levante ao desembarque;
- a armazenagem de mercadorias e a prestação de outros serviços complementares;
- a movimentação de contentores, quando estes constituem complemento de carga do navio.

Petróleos de Portugal PETROGAL, S.A. (5 e 5-VC)

A exploração dos Terminais de Petroleiros e Oceânico de Leixões está atribuída a esta empresa, mediante um contrato de concessão de uso privativo, pelo prazo de 25 anos que se iniciou em 2006.

O Terminal de Petroleiros está construído sobre o quebra-mar exterior (700 m de comprimento e altura de 15 m acima do nível do mar), servindo também de protecção à entrada no porto e ligado com a Refinaria de Leça da Palmeira através de oleodutos e gasodutos.

Os três postos de acostagem que o compõem são:


- Posto A (-15m ZHL) para ramas de petróleo e produtos refinados diversos;
- Posto B (-10 ZHL) para ramas de petróleo e produtos refinados diversos, gases liquefeitos e produtos aromáticos;
- Posto C (-6m ZHL) para gases de petróleo liquefeitos, produtos refinados diversos e produtos aromáticos.

A Petrogal tem a obrigação de prestação de serviços a terceiras entidades que possuam tubagens ligando os seus parques de armazenagem ao Terminal.

O Terminal Oceânico está localizado no exterior do Porto de Leixões, na área de domínio público marítimo sob a jurisdição da APDL, sendo propriedade da Petrogal e dispondo de um ponto único de amarração. A utilização do Terminal Oceânico tem em vista a movimentação de petróleo bruto.



A exploração dos Terminal de Asfalto de Viana do Castelo está atribuída a esta empresa, mediante um contrato de concessão de uso privativo, pelo prazo de 25 anos que se iniciou em 1997.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O Terminal de receção, armazenagem e distribuição de asfaltos com uma capacidade total de 6.256 m³ distribuída por 15 tanques. É abastecido por duas tomadas de cais de 6" de diâmetro, situadas no setor 1 do Cais Comercial.



SDL - Silos de Leixões, Unipessoal, Lda.


Com Contrato de Concessão de serviço público, pelo prazo de 25 anos, que se iniciou em 2007. Silos de Leixões procede à armazenagem a granel de cereais e sucedâneos.

O Silo de Leixões é composto por um silo de armazenagem, um silo de expedição, uma torre de elevação e um armazém horizontal perfazendo uma capacidade de armazenagem de 100.000 toneladas.

Terminal Roll-On/Roll-Off – porto de Viana do Castelo

Constituído por um cais de atracação com 245 metros de comprimento, equipado com um pontão flutuante e uma ponte de ligação ao terra pleno. Este, destinado ao estacionamento de atrelados e contentores, possui uma área com 3.000 m². O terminal permite operar navios com rampa lateral, rampa de proa ou de popa, em qualquer situação de maré.



	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

CECISA – Comércio Internacional, S.A., no porto de Viana do Castelo

A exploração do Terminal de Cimento está atribuída a esta empresa, mediante uma licença, pelo prazo de 10 anos que se iniciou em 2010.

Terminal de receção de cimentos e cinzas, ocupa uma área global de 12.900 m², sendo constituído por um armazém de ensacagem / armazenagem, com área de cerca de 3.800 m² e por 16 silos, com uma capacidade total de 49.800 toneladas de armazenagem.

SECIL – Companhia Geral de Cal e Cimento, S.A., no porto de Viana do Castelo

A exploração do Terminal de Cimento está atribuída a esta empresa, mediante uma licença, pelo prazo de 30 anos que se iniciou em 1990.

Terminal de receção, armazenagem e distribuição de cimento a granel, com uma capacidade de armazenagem de 6.000 toneladas. É abastecido por uma tomada de cais de 10" situada no sector 4 do Cais Comercial.

Agentes de Navegação

São considerados agentes de navegação as sociedades comerciais com o objetivo de dar cumprimento, em seu nome e por conta e ordem de armadores ou transportadores marítimos, a disposições legais ou contratuais, executando e promovendo junto das autoridades portuárias, ou de outras entidades, os actos ou diligências relacionados com a estadia dos navios que lhes estejam consignados.


Transitários

A atividade transitária consiste na prestação de serviços de natureza logística e operacional que inclui o planeamento, o controlo, a coordenação e a direcção das operações relacionadas com a expedição, recepção, armazenamento e circulação de bens ou mercadorias

Tais atividades abrangem os seguintes domínios de intervenção:

- Gestão dos fluxos de bens ou mercadorias;
- Mediação entre expedidores e destinatários, nomeadamente através de transportadores com quem celebre os respetivos contratos de transporte;
- Execução dos trâmites ou formalidades legalmente exigidos, inclusive no que se refere à emissão do documento de transporte unimodal ou multimodal.

Por último se refere, que a aposta numa oferta de serviços de valor acrescentado e no nível de capacidade de serviços no domínio do turismo de cruzeiros, está patenteada no volume de investimento disponibilizado para a criação da Plataforma Logística de Leixões com uma área de implantação de 60ha distribuída em dois pólos e no novo Terminal de Cruzeiros com capacidade para navios até 300 metros de comprimento, constituindo ambos os maiores projetos recentemente realizados.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015


Âmbito organizacional da gestão de risco

É objetivo o desenvolvimento de um modelo de gestão de risco transversal à organização, também designado por gestão de risco empresarial. Para este fim foi seguida o COSO II o qual define risco empresarial da seguinte forma:

“A gestão de risco empresarial (“Enterprise Risk Management” ou ERM) é um processo conduzido pela gestão de topo e envolvendo outros profissionais da organização, com aplicação direta na definição da estratégia da empresa, concebido para identificar potenciais eventos que podem afetar a organização, e gerir os correspondentes riscos para que estes se mantenham dentro de níveis aceitáveis pela organização, alcançando uma razoável garantia sobre o cumprimento dos objetivos da organização.”

Identificar e entender os objetivos da organização e os objetivos dos departamentos e Unidades Orgânicas é fundamental para garantir que todos os riscos significativos são capturados. A identificação dos objetivos no contexto de gestão do risco da APDL deverá ser efetuada com base em documentação formal proveniente de entidades internas e externas, da qual se apresentam alguns exemplos abaixo:

- Relatório e contas (2013);
- Relatórios de Balanced Scorecard;
- Recomendação do Conselho da Prevenção da Corrupção, de 01 de julho de 2009 – Planos de Gestão de Riscos de Corrupção e Infrações Conexas;
- Um oceano de oportunidades - Uma política marítima integrada para a União Europeia (publicação das Comunidades Europeias, 2008);
- Bases para a Estratégia de Gestão Integrada da Zona Costeira Nacional (relatório do grupo de trabalho nomeado por Despacho nº 19 212 /2005 do Ministro do Ambiente, do Ordenamento do Território e do Desenvolvimento Regional 2006);
- Para uma futura política marítima da União: Uma visão europeia para os oceanos e os mares (Livro Verde) (publicação das Comunidades Europeias, 2008);
- Orientações estratégicas para o sector marítimo portuário (publicado pela Secretaria de Estado dos Transportes, Ministério das Obras Públicas, Transportes e Comunicações);
- Política marítimo-portuária rumo ao século XXI (Livro Branco) (RCM nº82/1998 de 10 de Julho)
- Estratégia Nacional para o Mar (RCM n.º 128/2005, de 10 de Agosto)

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Critérios para identificação e avaliação de riscos

Um outro aspecto que é abordado na fase de estabelecer o contexto consiste em definir um conjunto de critérios de gestão de risco que permitam a análise, avaliação e posterior tratamento do risco. Tipicamente são identificados os seguintes tipos de critérios, sem os quais não é possível avaliar o risco de uma forma adequada:

- Categorização e classificação do risco;
- Avaliação / medição de probabilidade e impacto do risco;
- Classificação do nível de controlo;
- Aceitação do risco e indicadores de alerta de risco;
- Estratégias para tratamento de risco;
- Identificação de interlocutores para os riscos

A definição de cada um destes critérios é apresentada mais à frente no capítulo 4 deste documento.

3.2 Fase 2 – Identificar riscos


O principal objetivo desta fase consiste no desenvolvimento de uma lista de eventos que possam ter um impacto adverso ou favorável para a concretização dos objetivos identificados na fase 1 “Estabelecer contexto”.

Conceptualmente, e de acordo com a norma ISO 31000, risco pode ser definido como o “efeito da incerteza nos objetivos”. Neste contexto, é necessário definir o que se entende por “efeito”, “incerteza” e “objetivos”, tendo ainda como referência a norma ISO 31000:

- Efeito – Desvio face ao espectável (positivo ou negativo);
- Incerteza – Representa a falta de informação relacionada com o entendimento ou conhecimento de um evento, as possíveis consequências e a sua possibilidade de ocorrência; e
- Objetivos – Podem ser de diversos aspetos (e.g. financeiros, imagem, saúde) e atuar a vários níveis (e.g. organização, projeto, serviço).

Para identificação dos riscos existem diversas abordagens possíveis, cuja aplicação dependerá do contexto da gestão de risco. Algumas das técnicas normalmente utilizadas são:

- **Brainstormings ou workshops** – sessões com colaboradores da organização, nas quais devem ser consideradas diferentes perspetivas e incorporadas diversas experiências. Usualmente, esta é a abordagem preferida para a identificação de riscos numa primeira iteração do processo de gestão de risco;

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- **Mapas de riscos** – Os mapas de riscos constituem uma fonte importante na identificação de possíveis riscos a que a organização está exposta. Estes mapas de riscos podem ser provenientes de exercícios de identificação de risco efetuados por outras organizações similares ou provenientes de mapas de riscos genéricos a todas as organizações normalmente disponibilizados por empresas que prestam serviços de consultoria nesta área. Uma análise criteriosa deverá ser sempre efetuada de modo a validar a pertinência, validade e aplicabilidade dos riscos presentes nos mapas utilizados;
- **Questionários** – estes questionários deverão ser usados em entrevistas com os responsáveis de áreas ou departamentos permitindo a auto-identificação de riscos e das respetivas causas, fatores de risco ou consequências;
- **Benchmarking de indústria** – esta técnica consiste em obter, através de consulta a informação pública, os riscos a que outras organizações similares consideram estar expostas. Nestas abordagens deverão ser consideradas as especificidades de cada organização, validando assim a aplicabilidade dos riscos. Uma vez que a informação pública, normalmente não evidencia o nível de risco, este método é mais utilizado para validação do universo de riscos aplicáveis à organização;
- **Análise de cenários e hipóteses** – Estas técnicas são utilizadas para identificação de riscos externos ou estratégicos, uma vez que nestes casos o contexto é menos claro e mais difícil de definir.

Os resultados a obter nesta fase são:

- **Dicionário de Riscos** – Lista dos riscos identificados, agrupados pelas respetivas categorias e suas descrições; e
- **Mapa de risco** – Diagrama que ilustra os riscos distribuídos de acordo com as classes e categorias definidas.

3.3 Fase 3 – Analisar riscos


Esta fase tem dois principais objetivos:

- 1) Identificar as causas que podem levar à ocorrência do risco e fatores que contribuem para um aumento da vulnerabilidade do risco (aumento da probabilidade) ou um aumento das consequências (aumento do impacto); e
- 2) Identificar os Controlos / medidas de mitigação que podem contribuir para mitigar o risco.

As causas, também designadas por eventos de risco, condicionam a ocorrência do risco, ou seja, são determinantes para a avaliação da probabilidade de ocorrência do risco. Quanto aos controlos, permitem avaliar formas de mitigar o impacto do risco (controlos que atuam sobre as consequências) e de mitigar a probabilidade da sua ocorrência (controlos que atuam sobre as causas / eventos de risco).

Os resultados a obter nesta fase são:

Elaborado: AIQ Data: 14/07/2015	Aprovado: CA Data: 16/07/2015	Página 21 de 47
------------------------------------	----------------------------------	-----------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- **Fatores de risco** – Identificação dos principais fatores de risco que contribuem para cada um dos riscos identificados; e
- **Controlos / medidas de mitigação** – Identificação de controlos “típicos” ou existentes para cada um dos riscos identificados. Não é objetivo desta fase avaliar os controlos quanto à existência, desenho, implementação e eficácia operacional.

Fatores de risco

A identificação dos fatores de risco deverá ter em consideração as seguintes tipologias de fatores:

- **Fatores internos** – Os fatores de risco internos estão relacionados com a própria organização, nomeadamente ao nível das “pessoas”, “infra-estruturas”, “tecnologias” e “processos”. Neste particular consideram-se fatores que espelham debilidades a um ou mais níveis;
- **Fatores externos** – Os fatores de risco externos não se encontram sobre o controlo direto da organização, podendo estar relacionados com “economia”, “meio ambiente”, “política”, “enquadramento social”, entre outros;
- **Fatores “de passado”** – Fatores relacionados com eventos ocorridos na organização ou em organizações similares; e
- **Fatores “de futuro”** – Fatores que utilizam previsões sobre o futuro para estimar a sua influência no risco. Podem estar relacionados, por exemplo, com estudos de evolução demográfica ou de evolução do mercado.


A identificação dos fatores de risco deverá ter ainda em consideração:

- Factores de risco que afetam mais do que um risco; e
- Riscos que atuam como fatores de risco num outro risco.

A identificação dos fatores de risco constitui uma ajuda preciosa para os interlocutores envolvidos no processo de Gestão de Risco, uma vez que estimula a sua sensibilidade para a avaliação dos riscos.

Controlos / medidas de mitigação

Os controlos, ou atividades de controlo, são as políticas e os procedimentos que auxiliam o processo de gestão do risco. Encontram-se a todos os níveis da organização, transversalmente a todas as áreas e funções e fazem parte dos processos da organização para alcançar os seus objetivos de negócio. Os controlos incluem uma variedade de atividades como por exemplo aprovação, verificação, reconciliação, revisão ou monitorização.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O conceito estrito de controlos prevê dois tipos diferentes que se distinguem pela sua atuação perante os riscos que se propõem mitigar:

- **Controlos preventivos** – São controlos que atuam preventivamente sobre os riscos e cujo objetivo é reduzir as suas vulnerabilidades ou probabilidade de ocorrência. Usualmente estes controlos diminuem o número de eventos que podem originar o risco reduzindo assim a probabilidade de ocorrência do risco (e.g. controlo de acessos às instalações, relativamente ao risco de acidentes de trabalho), diminuem a exposição ao risco através da eliminação ou redução dos fatores de risco reduzindo assim as vulnerabilidades que podem originar a ocorrência do risco (e.g. uso obrigatório de capacete de proteção, ainda relativamente ao risco de acidentes de trabalho);
- **Controlos detetivos** – São controlos que atuam relativamente sobre os riscos cujo objetivo é a redução do impacto causado pela ocorrência do risco. O facto de serem reativos perante o risco não significa que a sua atuação dependa da ocorrência do risco, na realidade estes controlos são realizados mesmo sem materialização do risco (e.g. sistema de deteção de incêndios relativamente ao risco de incêndio). Tipicamente, estes controlos têm associadas ações corretivas sempre que “detetam” a ocorrência do risco (algumas vezes designados por controlos corretivos) cujo objetivo é atuar caso seja detetada a ocorrência real do risco (e.g. sistema de extinção de incêndio ainda relativamente ao risco de incêndio).

Estas definições não devem limitar a identificação de controlos. O que é fundamental na identificação dos controlos é avaliar se existe uma contribuição efetiva para a mitigação do risco.


Apesar de alguns controlos atuarem especificamente sobre um determinado risco ou categoria de riscos, muitas vezes existe sobreposição da sua atuação. Por exemplo, um controlo a nível operacional também tem influência ao nível do *reporting* ou *compliance*.

Um aspeto igualmente importante na identificação dos controlos para mitigação do risco consiste em avaliar se existe um excesso de controlos, quer por sobreposição do seu objetivo (e.g. controlos redundantes, ou controlos realizados por áreas diferentes da organização) quer por um nível de controlo excessivo face ao nível de risco. Nestes casos a identificação dos controlos fornece pistas para a otimização dos controlos através da eliminação ou consolidação de controlos.

Uma outra perspetiva sobre os controlos considera o seu nível de atuação, conforme definido no COSO II:

- **Políticas e procedimentos** – Em termos genéricos, as políticas definem o que deve ser feito e os procedimentos descrevem como deve ser feito. As políticas podem ter um carácter menos formal – políticas incutidas na organização mas não formalizadas – continuando a ser efetivas no seu efeito. Quanto aos procedimentos é necessário que os mesmos estejam sempre alinhados com as políticas – formais ou informais.
- **Controlos de Sistemas de Informação** – A maior dependência dos sistemas de informação torna necessária a existência de controlos específicos. Neste âmbito consideram-se usualmente dois tipos de controlos, os controlos aplicacionais e os controlos gerais.

Os controlos aplicacionais são concebidos para assegurar a totalidade, rigor, autorização e validade do processo de captura, tratamento e partilha de dados.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Os controlos gerais atuam transversalmente a todo o ambiente de tecnologias de informação – desde os computadores centrais até aos computadores pessoais – e podem existir ao nível da gestão dos sistemas de informação, infra-estruturas tecnológicas, segurança lógica e física e desenvolvimento / manutenção dos sistemas.

Controlos aplicacionais	Controlos gerais
<ul style="list-style-type: none"> ▪ Tratamento e autorização de dados ▪ Recolha / introdução de dados ▪ Verificações quanto à validade, totalidade e correção dos dados ▪ Isenção, validade e integridade do processamento ▪ Reconciliações e tratamento de erros ▪ Integridade e autenticidade da informação 	<ul style="list-style-type: none"> ▪ Segurança lógica e gestão de acessos ▪ Gestão das operações de tecnologias de informação ▪ Segurança física ▪ Gestão de alterações e desenvolvimento

Abordagens utilizadas para analisar riscos


Na identificação dos fatores de risco e dos controlos é muito importante o conhecimento do negócio e da realidade particular da Empresa e o conhecimento de ocorrências passadas de eventos de risco. Torna-se assim essencial a participação ativa das Unidades Orgânicas neste exercício.

Por outro lado, e não menos importante, é benéfica experiência na realização de exercícios similares, tornando-se assim fulcral a participação da área de Auditoria Interna neste exercício. Este aspeto é ainda mais relevante na identificação dos controlos / medidas de mitigação.

A identificação dos fatores de risco deverá ser efetuada utilizando preferencialmente as seguintes abordagens:

- **Brainstorming** – Discussão alargada sobre as potenciais causas para cada um dos riscos, tendo sempre o cuidado de restringir essas causas à realidade da APDL (e.g. empresas, localizações);
- **Entrevistas individuais com a gestão** – Estas conversas, que podem ser efetuadas simultaneamente com a identificação dos riscos. Face à técnica do brainstorming, esta abordagem tem a vantagem de poder ser mais direcionada e estruturada, sendo ainda de realçar a inexistência de influência de interlocutores de outras áreas;
- **Eventos passados** – Identificação de eventos ocorridos no passado e que podem indiciar uma probabilidade elevada de ocorrência futura.

Quanto à identificação de controlos, também pode ser efetuada de várias formas as quais deverão ser ponderadas aquando de cada exercício de análise dos riscos. Um dos fatores que determina a


	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

forma de identificar os controlos é o grau de maturidade do modelo de gestão de risco. Quanto maior for a maturidade deste modelo maior deverá ser o detalhe e granularidade na identificação dos controlos. Pelo contrário, no início da evolução do modelo de gestão de risco deverão ser utilizados métodos que identifiquem os principais controlos os quais podem agregar um conjunto de controlos.

Algumas das abordagens possíveis para a identificação dos controlos são:

- **Entrevistas individuais com a gestão** – Este método representa o primeiro passo para identificação dos principais controlos existentes. Nesta fase não é pretendido obter detalhe sobre as características dos controlos, mas apenas obter uma perceção do nível de controlo existente. Estas entrevistas poderão ser realizadas conjuntamente com a fase de avaliação dos riscos;
- **Questionários de controlos** – Numa segunda iteração do processo, necessariamente mais rigorosa e dirigida aos riscos, poderão ser emitidos questionários direcionados aos interlocutores identificados para cada risco. Este método deverá permitir a identificação não só dos controlos existentes como também das principais oportunidades de melhoria ou lacunas de controlo;
- **Benchmarking e melhores práticas** – O recurso às melhores práticas de controlo e a outras organizações onde os riscos se manifestem de forma idêntica consiste num método que permite, por um lado, estimular a organização para a existência de alguns controlos, mas sobretudo permite a identificação de oportunidades de melhoria e lacunas de controlo;
- **Consulta a manuais de procedimentos e outra documentação** – Numa fase posterior do modelo de gestão de risco, a que corresponderá uma maior maturidade, poderá ser efetuada uma identificação mais pormenorizada dos controlos através de consulta a manuais de procedimentos, manuais de operação ou outra documentação interna à organização;
- **Levantamento de processos** – Este método, apesar de não ser orientado diretamente para cada um dos riscos – em vez disso é orientado ao processo – permite identificar controlos incutidos na organização e que não se encontram refletidos em documentação processual ou operacional. Este método não é normalmente utilizado de forma exclusivamente com o objetivo de identificar os controlos, devido ao peso que lhe está associado; e
- **Manuais de controlo interno** – Esta abordagem consiste em recorrer a manuais de controlo interno existentes na organização, em particular na área de Auditoria Interna. Permite uma identificação de elevada granularidade, sendo assim associada a fases de maior maturidade do modelo de gestão de risco.

As duas primeiras abordagens descritas acima pressupõem a consulta aos interlocutores considerados como os que mais intervenção têm na gestão de cada um dos riscos. Esta abordagem não impede que um determinado controlo identificado no contexto de um risco específico não possa ser considerado também para mitigação de outro risco.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

3.4 Fase 4 – Avaliar riscos

A avaliação dos riscos tem como objetivo ajudar na definição de prioridades e tomada de decisões para o tratamento dos riscos identificados. Esta avaliação expressa o risco através da combinação de dois componentes: impacto e a probabilidade.

O impacto mede as consequências diretas e indiretas para a organização, como por exemplo perdas financeiras ou danos na reputação e imagem. Este poderá ser avaliado em função de quatro fatores:

- 1) **Capacidade de previsão dos eventos de risco** – uma menor capacidade conduz a um aumento do impacto potencial do risco;
- 2) **Capacidade de atuação perante um evento de risco** – uma menor capacidade conduz igualmente a um aumento do impacto potencial do risco;
- 3) **Abrangência dos eventos** – eventos locais têm menor impacto do que eventos transversais;
- 4) **Duração do evento** – quanto maior for a duração do evento maior será o impacto associado ao mesmo.

A probabilidade reflete o maior ou menor grau de certeza quanto à ocorrência do risco identificado com um horizonte temporal previamente definido. Este horizonte temporal, varia tipicamente entre 3 e 5 anos, não devendo ser estendido muito para além dos 5 anos, pois a vulnerabilidade aumentaria para valores perto do máximo para muitos dos riscos, nem deverá ser reduzido para menos de 3 anos, uma vez que esta poderia atingir valores insignificantes em muitos casos.


A probabilidade mede ainda a vulnerabilidade do risco que se está a analisar. A título de exemplo, a probabilidade de se perpetrar um furto a uma residência não aumenta com o número de janelas da residência ou com o andar em que se localiza, contudo, qualquer um destes fatores aumenta a vulnerabilidade face a furtos.

A avaliação do nível de impacto e da vulnerabilidade para cada um dos riscos poderá seguir uma abordagem qualitativa ou quantitativa.

Avaliação qualitativa do nível de risco

Na maior parte das situações, e em particular quando a aplicação do modelo de gestão de risco ainda se encontra numa fase inicial, uma avaliação qualitativa do nível de risco é suficiente para o caracterizar. Esta abordagem não significa um menor rigor na análise, podendo mesmo ser a única forma de avaliar o nível de risco para alguns riscos em particular. Os métodos a utilizar para a avaliação qualitativa incluem:

- Entrevistas individuais com os principais intervenientes / agentes envolvidos nos riscos;
- *Workshops* com grupos multi-disciplinares para riscos que abranjam várias áreas ou departamentos da organização;

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- Indicadores qualitativos inerentes ao negócio (e.g. necessidade de peças estratégicas para manutenção, número de reclamações rececionadas, índices de satisfação dos consumidores);
- Questionários de avaliação de risco (em papel ou formato eletrónico); e
- Análise da inter-relação e interdependência de riscos.

Avaliação quantitativa do nível de risco

À medida que o processo de gestão de risco se torna mais maduro e estável, a abordagem quantitativa deverá ser progressivamente adotada, inicialmente como complemento aos métodos qualitativos, e por fim sendo o suporte preferencial para a avaliação do nível de probabilidade e impacto de cada risco. Alguns dos métodos normalmente utilizados na avaliação quantitativa são:

- Análises estatísticas de ocorrências de eventos de risco;
- Indicadores de gestão; e
- Simulação e modelação de informação histórica sobre ocorrência de eventos de risco.

A avaliação (qualitativa ou quantitativa) da vulnerabilidade e impacto de cada um dos riscos resultará numa matriz de riscos que irá permitir ter uma visão global do posicionamento dos mesmos.


Risco inerente e risco residual

Numa primeira fase, e qualquer que seja a abordagem para avaliação do risco, as medidas existentes para os mitigar não deverão ser consideradas, pois importa medir o risco inerente, ou seja a exposição da organização ao risco, resultante do seu contexto interno e externo. Assim, o risco inerente deverá ser avaliado independentemente das medidas que existam para a sua mitigação ou controlo.

Sem esta primeira avaliação, a organização perderia a capacidade de saber qual a sua exposição ao risco, no caso de falha das medidas de mitigação existentes.

Adicionalmente, a avaliação do risco inerente permite ter uma melhor perspetiva sobre o nível de controlo que deverá existir, uma vez que riscos com baixa probabilidade e impacto em termos inerentes, poderão não requerer medidas de mitigação. Desta forma evidenciam-se medidas de mitigação ou controlo desnecessárias ou supérfluas.

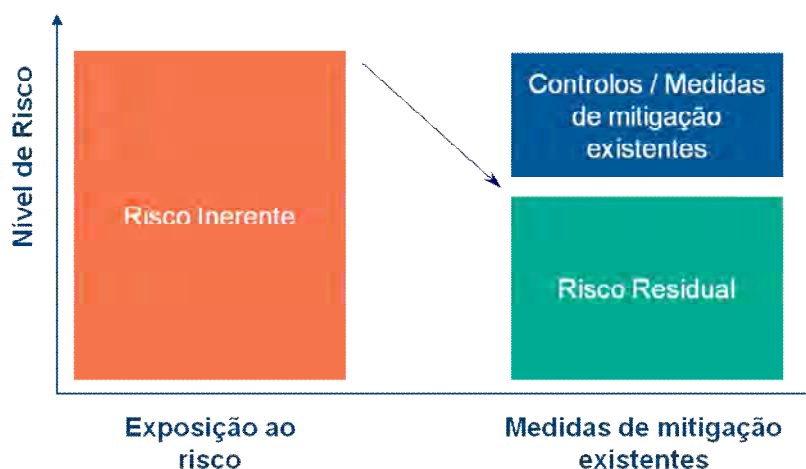
Numa fase posterior, deverão ser avaliadas as medidas de mitigação existentes para cada um dos riscos, obtendo-se uma matriz de risco residual que representa a exposição ao risco em função da existência e efetividade das medidas de mitigação, ou seja da adequação do nível de controlo. De referir que em algumas situações não é possível medir a adequação do nível de controlo existente, nomeadamente para alguns dos riscos de cariz estratégico (e.g. risco da envolvente económica e

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

financeira, risco político). Nestes casos o risco residual é avaliado tendo em conta estratégias da Gestão (e.g. acompanhamento da evolução política, estudos de mercado, relações institucionais).

De notar que o âmbito de avaliação dos controlos, ou medidas de mitigação, poderá não abranger a totalidade dos riscos identificados. Este é um processo iterativo e periódico, para o qual deverão ser definidas prioridades de análise para cada uma das iterações em função do nível de risco e das prioridades da Gestão.

A passagem do risco inerente para o risco residual é ilustrada na seguinte figura:




Os resultados a obter nesta fase são:

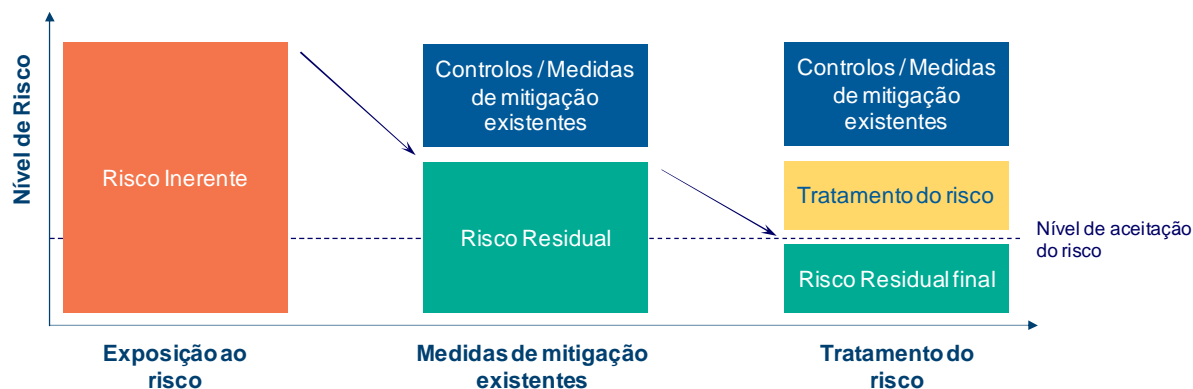
- Matriz de risco inerente;
- Avaliação do nível de controlo; e
- Matriz de risco residual.

3.5 Fase 5 – Tratar riscos

Esta fase tem como objetivo a elaboração de um plano de tratamento de riscos definindo as prioridades, o âmbito e o tratamento a efetuar para cada risco.

O racional subjacente a esta fase é ilustrado na seguinte figura:

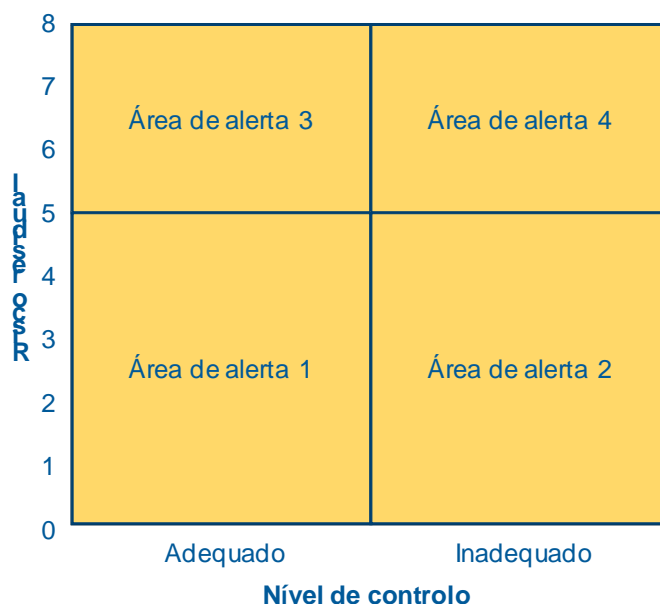
	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015




O tratamento de cada um dos riscos tem por base a matriz de risco residual resultante da fase anterior, sendo a decisão dos riscos a tratar tomada com base em dois critérios:

- Indicadores de alerta de risco; e
- Prioridades da Gestão.

O plano de tratamento permitirá assim mitigar o nível de risco residual para um nível considerado aceitável pela organização – “nível de aceitação do risco”. Neste contexto, os indicadores de alerta de risco são um precioso auxiliar para definir o plano de tratamento dos riscos, tal como é ilustrado na figura seguinte onde, a título exemplificativo, são definidas quatro áreas para tratamento de riscos:



A adequação do nível de controlo é um elemento importante na caracterização dos indicadores de alerta de risco pois permite aferir da necessidade de melhorar o nível de controlo existente.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

As decisão sobre o tratamento ou não tratamento de cada um dos riscos deverá ser documentada no plano de tratamento de riscos, justificando sempre que possível a opção tomada. Este aspeto é particularmente importante para os riscos que não serão tratados (por decisão da Gestão), apesar do indicador de alerta de risco evidenciar o contrário. A estrutura do plano de tratamento de riscos deverá assim distinguir entre:

- Riscos incluídos no nível de alerta que não necessitam de tratamento (risco residual baixo com nível de controlo adequado);
- Riscos incluídos no nível de alerta que necessitam de tratamento mas cuja decisão passa por não efectuar tratamento ou protelar o mesmo; e
- Riscos que serão tratados.

Como resultado desta fase, deverá ser criado um plano de tratamento de riscos, incluindo para cada um dos riscos:

- Prioridade de tratamento (em função do nível de alerta);
- Ações corretivas / de melhoria sobre o nível de controlo (em função do nível de alerta);
- Nível de aceitação para o risco (se for aferido para cada risco);
- Estratégia de tratamento para o risco (aceitar, eliminar, reduzir ou partilhar); e
- Plano de implementação.

3.6 Comunicação e consulta

A comunicação é um elemento importante em cada fase do processo de gestão de risco, uma vez que é essencial que todos os intervenientes e *stakeholders* deste processo entendam e partilhem das razões da necessidade de implementar determinadas ações ou de tomar determinadas decisões.


É crucial seguir uma abordagem de comunicação por toda a organização, transversalmente a todos os departamentos e níveis de gestão.

Quanto à consulta, ela consiste no recurso a empresas de consultoria especializada na gestão de riscos para que seja utilizado o seu capital de conhecimento em qualquer uma das fases do processo. A sua colaboração deverá ser ponderada sempre que se considere útil para o processo o aporte de conhecimento especializado ou quando seja necessário complementar as competências internas.

Plano de comunicação

A comunicação com os intervenientes no processo de gestão de risco deverá ocorrer durante todas as fases previstas no modelo de gestão de risco. Contudo, também neste particular a comunicação deverá evoluir a par com o aumento de maturidade do modelo de gestão de risco. Não poderá ser

Elaborado: AIQ Data: 14/07/2015	Aprovado: CA Data: 16/07/2015	Página 30 de 47
------------------------------------	----------------------------------	-----------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

demasiado ambiciosa nas primeiras iterações do modelo mas os princípios subjacentes deverão ser sempre garantidos.

Neste contexto, torna-se relevante definir os vários grupos aos quais deverão ser efetuadas comunicações:

- Administração
- Direções
- Interlocutores de risco (incluindo os facilitadores / dinamizadores do processo de gestão de risco)
- Colaboradores da organização (não incluídos nos grupos acima)
- *Stakeholders* (externos à organização)

Para cada um dos grupos acima identificados deverão ser definidos conteúdos, formatos e momentos da comunicação a efetuar de forma a gerir expectativas, definir responsabilidades de pessoas e grupos entre outros aspetos importantes.

A nível interno deverá ser comunicada a filosofia da organização quanto à gestão de risco, a abordagem adotada e a delegação de competências definida. Deverá ficar claro para todos os *stakeholders* internos:


- A importância e efeitos da gestão de risco para a organização;
- Os níveis de aceitação do risco definidos pela organização;
- Uma linguagem comum relativa ao risco; e
- As responsabilidades internas no processo de gestão de risco.

Uma comunicação eficiente dos princípios subjacentes à gestão de risco irá permitir à organização reagir a acontecimentos inesperados focando-se não apenas os efeitos mas também nas suas causas. Por outro lado, irá incutir na organização uma consciência para os efeitos e responsabilidades noutras áreas face a acontecimentos adversos, por oposição à lógica mais comum de “silos” departamentais de responsabilidade.

Outras das vantagens obtidas com uma comunicação eficiente são:

- Conhecimento comum a todas os colaboradores dos riscos a que a organização está exposta;
- Identificação precoce de focos de problemas (fatores de risco); e
- Comunicação no sentido ascendente, descendente e transversal à organização.

Neste aspecto da comunicação, os facilitadores da gestão de risco assumem um papel de grande importância ao estabelecerem os canais de comunicação apropriados em todos os sentidos dentro da

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

organização (entre a administração e o acionista Estado, entre unidades orgânicas, entre as unidades orgânicas e a administração, entre a organização e a Auditoria Interna).

A nível externo a comunicação sobre a gestão de risco é importante que ocorra também nos dois sentidos:

- Obter dos *stakeholders* externos a informação necessária para alimentar a gestão de risco a qual pode influenciar os níveis de aceitação do risco da organização (e.g. maiores exigências ambientais dos *stakeholders* locais originam uma redução do nível de aceitação do risco ambiental);
- Alinhamento dos níveis de aceitação do risco com os parceiros de negócio (e.g. concessionários) de modo a garantir que a organização não incorpora demasiado risco proveniente destes;
- Incorporação de informação proveniente de entidades externas no modelo de gestão do risco (e.g. incorporação de resultados de auditorias externas);
- Comunicação de resultados a *stakeholders*, reguladores, acionista (Estado) de modo a que seja obtido um entendimento comum das circunstâncias e riscos da organização.


Todos estes exemplos de comunicação devem ocorrer atempadamente, com informação atualizada e pertinente.

Comunicação de resultados

A comunicação de resultados deverá ser efetuada no final de cada ciclo do processo de gestão de risco, de acordo com o grupo a que se destina a informação a comunicar e com o nível de maturidade do processo.

A tabela abaixo ilustra alguns exemplos de iniciativas de comunicação relativas à primeira iteração do processo de gestão de risco:

Grupo	Conteúdo	Meio de comunicação (exemplos)
Administração, Unidades orgânicas	<ul style="list-style-type: none"> • Dicionário de riscos (incluindo fatores de risco, principais controlos e oportunidades de melhoria) • Mapa de risco inerente (completo) • Riscos de elevada prioridade 	e-mail, intranet
Colaboradores	<ul style="list-style-type: none"> • Mapa de risco inerente (completo) • Descrição das principais medidas de mitigação existentes • Descrição das principais oportunidades de 	e-mail, apresentação presencial (e.g. evento da organização)

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

	melhoria (plano de mitigação do risco)	
Stakeholders (externos)	<ul style="list-style-type: none"> Principais riscos, respetivas medidas de mitigação existentes e medidas de mitigação em curso ou planeadas. 	Relatório e Contas


3.7 Monitorização e revisão

A monitorização e revisão periódica do processo de gestão de risco é essencial para garantir que a avaliação dos riscos realizada continua correta e se mantém pertinente. Adicionalmente, os fatores que afetam a probabilidade e impacto dos riscos estão sujeitos a mudança, afetando desta forma o custo e viabilidade das opções de tratamento do risco, tornando necessária a repetição do processo de gestão de risco com um caráter periódico.

A monitorização e revisão envolvem também a aprendizagem resultante do processo de gestão de risco, através da análise de eventos passados, dos planos de tratamento já implementados e dos seus resultados.

Em termos práticos, a monitorização e revisão consiste em:

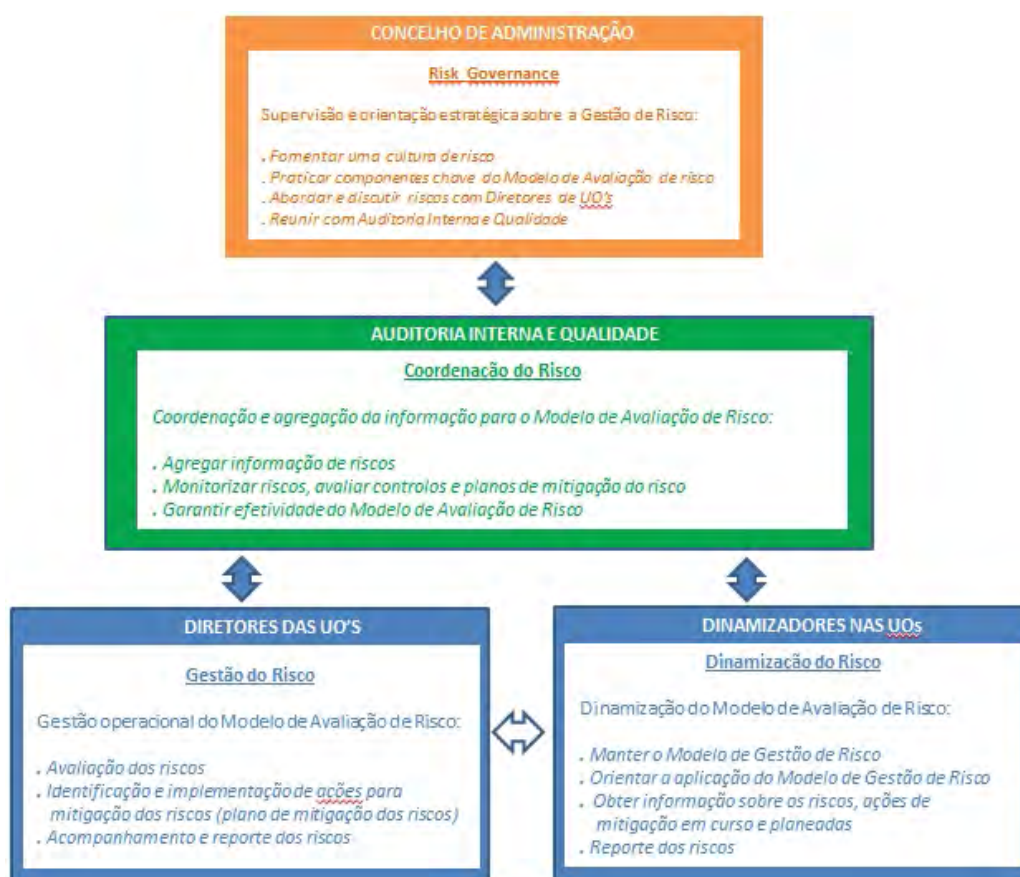
- Monitorizar de forma contínua através da medição e validação de determinados parâmetros de gestão que indiciam ocorrência de eventos de risco;
- Efetuar revisões pelos elementos da Gestão (usualmente denominadas *control self-assessments*); e
- Realizar auditorias internas ou externas. Tanto quanto possível, estas auditorias deverão testar os controlos / medidas de mitigação existentes, utilizando uma abordagem baseada no risco e procurando a adequação com padrões e requisitos legislativos.


	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

4. Critérios para gestão de risco

4.1 Funções e responsabilidades

O modelo de gestão de risco definido para a APDL assenta na seguinte estrutura de funções e responsabilidades:



	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

4.2 Organização dos riscos

A identificação dos riscos requer que exista uma estrutura que os agrupe e categorize de acordo com afinidades e características comuns. As normas instituídas para Gestão do Risco, nomeadamente o COSO II recomendam uma organização hierárquica dos riscos.


A Organização considerou as quatro classes recomendadas pelo COSO II e uma classe adicional para os riscos de Governação. Foram ainda consideradas dezasseis categorias de risco, conforme ilustrado na figura abaixo.



Classes de risco

As classes de risco agrupam os riscos de acordo com a sua natureza e influência na organização, permitindo identificar as principais causas subjacentes aos mesmos, alinhadas com a organização e o seu negócio. Foram definidas cinco classes de risco:

- **Governance** – *Governance* representa um conjunto de relações e estrutura organizacional através das quais os objetivos da organização são estabelecidos, e a forma de os avaliar e os meios para os alcançar são definidos. São considerados os valores corporativos de justiça, transparência, responsabilidade e os riscos associados à estrutura, políticas, procedimentos e responsabilidades relativamente aos quais são monitorizadas as decisões e orientações definidas para a organização.
- **Estratégia e Planeamento** – Riscos associados com a incapacidade da organização formular e / ou executar com sucesso a sua estratégia de negócio, em grande medida relacionada com planos para crescimento da organização (entrada em novos mercados, lançamento de novos produtos, criação de alianças / fusões, obtenção de sinergias proporcionadas por aquisições, introdução de novos modelos de negócio), com a introdução de novas plataformas tecnológicas ou a obsolescência de produtos ou serviços existentes.
- **Operacional / Infra-estrutura** – Riscos que impliquem perdas resultantes de processos internos, pessoas ou sistemas inadequados ou ineficientes, ou falhas de infra-estrutura essencialmente relacionadas com desempenho, proteção e utilização dos ativos da organização. Necessidades operacionais a médio e longo prazo deverão ser estimadas e

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

planeadas, e os respectivos recursos dimensionados e obtidos de forma a garantir o seu cumprimento de forma eficiente e a um custo competitivo.


- **Compliance** – Os objetivos de conformidade de uma organização prendem-se com o cumprimento de legislação, regulamentação e normas aplicáveis à sua atividade, incluindo políticas e normas externas e internas. As organizações deverão desenvolver a sua atividade e tomar as medidas que permitam cumprir com as leis e as regulamentações relevantes. Estes requisitos podem estar relacionados com mercados, *pricing*, impostos, ambiente ou recursos humanos. A conformidade da organização com as leis e regulamentações pode afetar significativamente (de forma positiva ou negativa) a sua reputação e imagem na opinião pública e no mercado.
- **Reporting** – Nesta classe incluem-se as preocupações relacionadas com a obtenção, compilação, apresentação e divulgação de informação financeira e não-financeira aos *stakeholders* da organização. A divulgação de informação pode variar desde relatórios internos para a gestão até a relatórios externos exigidos pelas leis locais ou organismos de regulação. Falhas no processo obtenção, análise e apresentação de informação interna ou externa relevante, pode resultar na divulgação de informação financeira (e operacional) incorreta para o mercado.

Categorias de risco

A utilização de categorias de risco permite que dentro de uma mesma classe os riscos estejam agrupados de acordo com afinidades existentes entre eles. As categorias definidas pela APDL foram as seguintes:

Classe Governance


Categoria	Descrição da Categoria
Corporate Governance	<i>Corporate governance</i> reflete-se num conjunto de processos, políticas, leis, normas que afetam a forma como a organização é gerida, administrada ou controlada. Alguns elementos chave numa boa <i>corporate governance</i> incluem a honestidade, confiança e integridade, transparência, valorização do mérito, responsabilidade e responsabilização, respeito mútuo e comprometimento perante a organização. Em particular, uma boa <i>corporate governance</i> destaca o papel dos executivos de topo na execução e incentivo de práticas honestas e éticas, especialmente no que diz respeito à atuação perante conflitos de interesses e divulgação de informação financeira. Falha da organização em colocar em prática boas medidas de <i>corporate governance</i> potencia a execução de atos ilícitos, ou não éticos por parte dos seus colaboradores a todos os níveis, podendo resultar na divulgação fraudulenta de informação.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Categoria	Descrição da Categoria
Ética	A existência de medidas e programas dedicados à ética e conformidade permite sustentar os objetivos da organização, definir fronteiras para comportamentos lícitos e éticos e estabelece uma forma de alertar a gestão sempre que a organização se aproxima ou transpõe obstáculos / fronteiras (e.g. fraude interna, não-conformidades legais, comportamentos não-éticos) que condicionam ou impedem o cumprimento dos seus objetivos de negócio. Falha da organização em definir e implementar medidas e programas de ética de forma eficiente podem ter como consequência a organização não conseguir promover e incentivar uma cultura de confiança, responsabilização e / ou integridade conduzindo à perpetração de ações fraudulentas. A organização deverá considerar os programas de ética como parte integrante do seu negócio e incentivar junto dos seus colaboradores a divulgação de violações detetadas.

Classe Estratégia e Planeamento


Categoria	Descrição da Categoria
Responsabilidade Social e Sustentabilidade	As preocupações ambientais das organizações, nomeadamente em relação ao impacto que provocam no ambiente, são cada vez maiores. Como consequência, as organizações têm vindo a iniciar esforços para se tornarem mais ambientalmente responsáveis. A responsabilidade e sustentabilidade das organizações representa um processo contínuo de melhoria das operações no sentido de garantir disponibilidade de recursos a longo termo, sensibilidade social e transparência no relacionamento com os consumidores, parceiros de negócio e a comunidade.
Fatores Externos	Fatores externos como sejam condições políticas, económicas / de mercado, sociais, tecnológicas, legais ou regulamentares e ambientais, constituem ameaças às organizações as quais não podem ser diretamente controladas por estas. Apesar de inesperadas e fora do controlo das organizações, acontecem com regularidade suficiente para se poderem considerar como bastante prováveis.
Estratégia	A estratégia envolve o planeamento a longo prazo de ações da organização para alcançar os seus objetivos de negócio. Pressionada por uma concorrência intensa e cada vez mais forte e por uma cada vez maior complexidade do negócio, as organizações devem considerar a perspetiva do risco aquando da formulação da estratégia para a organização. Esta abordagem ajuda na identificação e priorização de áreas de preocupação e na preparação de um plano estratégico de ação onde as responsabilidades, os resultados e os prazos são claramente definidos.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Categoria	Descrição da Categoria
Planeamento	O planeamento constitui uma base detalhada para alcançar os objetivos estratégicos das organizações. É um processo pelo qual as organizações definem as suas estratégias em termos práticos, e tomam decisões alocando recursos, capital e pessoas, para a prossecução dessas estratégias. A implementação dos planos pode ocorrer com apoio explícito da gestão, dos colaboradores e de todos os <i>stakeholders</i> da organização. Os riscos associados a esta atividade incluem falha no alinhamento funcional das estratégias e objetivos com a estratégia global da empresa. São também considerados os riscos de um ineficiente planeamento que possa comprometer os recursos da organização numa estratégia errada ou em negócios, projetos ou operações não rentáveis.

Classe Operacional / Infra-estrutura


Categoria	Descrição da Categoria
Gestão Administrativa	Os ativos empresariais incluem uma componente tangível (e.g. terrenos, fábricas, equipamentos e máquinas e instalações) e uma componente intangível (e.g. capital humano, propriedade intelectual). A incapacidade de proteger os ativos empresariais dos riscos ambientais (e.g. desastres naturais, incêndios), riscos de acesso (e.g. entradas não autorizadas, danos ou estragos) e a incapacidade de garantir a segurança pessoal dos colaboradores pode resultar em perdas para os ativos. A subutilização bem como uma inadequada manutenção dos ativos pode resultar em operações ineficientes. Com o cada vez maior ênfase no impacto ambiental e na sustentabilidade, a conceção de instalações, fábricas e equipamentos deve ter em consideração a eficiência, e o baixo impacto em termos de emissões e descargas para o meio ambiente de materiais e substâncias nocivas.
Gestão Financeira	A área financeira tem a preocupação de obter, atribuir e utilizar os recursos financeiros e também de utilizar as melhores ferramentas e análises para o processo de tomada de decisão. O objetivo primordial de uma função financeira é melhorar o valor da organização ao mesmo tempo que reduz os riscos financeiros da mesma. As organizações estão expostas aos riscos financeiros em áreas como por exemplo a estrutura de capitais, alocação de capitais, informação financeira ou taxas de juro.
Recursos Humanos	A área de recursos humanos inclui as políticas de recursos humanos, os processos e procedimentos e os sistemas que estão desenhados para suporte às suas atividades. Podem existir riscos derivados de fraquezas ou quebras nestas políticas, processos ou sistemas, comprometimento face e em apoio aos colaboradores da empresa, antes, durante e após o término do seu relacionamento com a organização.
Tecnologias de Informação	A utilização da tecnologia em todos os aspetos da evolução social e económica criou dependências críticas nas tecnologias de informação para iniciar, registar, mover e gerir a maior parte das ações relacionadas com transações

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Categoria	Descrição da Categoria
	económicas, informação e conhecimento. Os riscos de tecnologias de informação estão relacionados com incapacidade ou ineficiência da sua utilização no suporte à missão, visão e objetivos das organizações, na incapacidade de suportar os aspectos legais, ambientais, de qualidade e de segurança e de suportar os objetivos de reporte de informação e de gestão da mudança. Este risco também inclui ineficiências ao nível dos planos de continuidade do negócio, planos de recuperação em caso de desastre, e ineficiências ao nível operacional na condução dos processos da organização.
Legal	O risco legal está relacionado com falha nas infra-estruturas processuais, de sistemas e de recursos que suportam os requisitos de regulação e legais. Inclui ainda a protecção da propriedade intelectual e outros ativos intangíveis e a gestão de relações contratuais com pessoas ou entidades.
Desenvolvimento de Serviços e Investimentos	O desenvolvimento de serviços é o processo responsável pela introdução de novos serviços no mercado. Este processo inclui vários passos desde a formulação da ideia até à construção / disponibilização do serviço, podendo em última análise incluir ainda a fase de descontinuação dos serviços. As empresas consideram usualmente o desenvolvimento de produtos e serviços como a primeira etapa na oferta de novos serviços, integrado no processo estratégico global da gestão do ciclo de vida, utilizado para manutenção ou reforço da sua quota de mercado.
Marketing e Comunicação	A estratégia de vendas, marketing e comunicação de uma empresa não é coincidente com as alterações ao nível das exigências ambientais e do mercado. O risco está relacionado com a capacidade da organização em antecipar e satisfazer os requisitos e exigências do mercado e dos consumidores, desenvolver e comercializar produtos e serviços e entregá-los com a qualidade e a um preço que corresponda às expectativas dos consumidores, com o objetivo último de os reter como clientes.
Operações e Segurança	Os processos de operações incluem o planeamento, procurement, transporte e distribuição de produtos e serviços. Um processo eficiente deve disponibilizar produtos e serviços atempadamente, de qualidade e nas quantidades desejadas, a um preço correto. Falhas nos processos operacionais podem resultar em desajustes ou incorreções nas compras, desajustes nos processos de produção, de vendas ou de entrega tendo como consequência a incapacidade de obter os materiais correctos, de produzir de acordo com os planeamentos ou de entregar produtos ou serviços em condições deficientes.

Classe Compliance

Categoria	Descrição da Categoria
-----------	------------------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Categoria	Descrição da Categoria
Compliance	Os objetivos de conformidade de uma organização prendem-se com o cumprimento de legislação, regulamentação e normas aplicáveis à sua atividade, incluindo políticas e normas externas e internas. As organizações deverão desenvolver a sua atividade e tomar as medidas que permitam cumprir com as leis e as regulamentações relevantes. Estes requisitos podem estar relacionados com mercados, pricing, impostos, ambiente ou recursos humanos. A conformidade da organização com as leis e regulamentações pode afetar significativamente (de forma positiva ou negativa) a sua reputação e imagem na opinião pública e no mercado.

Classe Reporte

Categoria	Descrição da Categoria
Reporting	Nesta categoria incluem-se as preocupações relacionadas com a obtenção, compilação, apresentação e divulgação de informação financeira e não-financeira aos <i>stakeholders</i> da organização. A divulgação de informação pode variar desde relatórios internos para a gestão até a relatórios externos exigidos pelas leis locais ou organismos de regulação. Falhas no processo obtenção, análise e apresentação de informação interna ou externa relevante, pode resultar na divulgação de informação financeira (e operacional) incorreta para o mercado.

4.3 Critérios de probabilidade e de impacto dos riscos


Conforme anteriormente descrito, a incerteza dos eventos de risco pode ser medida em dois vectores: probabilidade e impacto. A probabilidade mede, de uma forma qualitativa, a possibilidade de ocorrência de um risco, enquanto que o impacto mede as suas consequências para a organização.

Uma vez que os riscos são identificados de acordo com os objetivos e estratégia da Empresa, é natural que sejam classificados num horizonte de curto a médio prazo (3 a 5 anos). No entanto, não é requerido que a classificação dos riscos seja exclusivamente limitada a este horizonte temporal uma vez que alguns deles têm influência nas orientações estratégicas da empresa ou em fatores externos de ocorrência muito espaçada no tempo.

Classificação da probabilidade


A classificação da probabilidade de ocorrência de um evento de risco é, por natureza, incerta. Contudo, torna-se necessário recorrer a métricas com maior ou menor grau quantitativo para a sua aferição. Algumas destas métricas poderão ser: o grau de conhecimento que existe do evento, o histórico de ocorrências, número de eventos de risco que concorrem para o risco, vulnerabilidade intrínseca da organização, no seu contexto interno ou externo, perante os eventos de risco, ou a análise de tendências do evento.

Elaborado: AIQ Data: 14/07/2015	Aprovado: CA Data: 16/07/2015	Página 40 de 47
------------------------------------	----------------------------------	-----------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O termo probabilidade não deverá ser entendido no seu estrito significado matemático. Deverá antes ser entendido num sentido mais lato, expressando simultaneamente a possibilidade de ocorrência de um evento e a vulnerabilidade da organização perante esse evento.


A seguinte tabela define a escala qualitativa de probabilidade usada para a classificação dos eventos de risco na APDL:


Classificação		Probabilidade
3 a 4	Muito elevado	
2 a 3	Elevado	
1 a 2	Médio	
0 a 1	Baixo	A probabilidade de ocorrência dos eventos de risco é baixa (e.g. histórico de eventos de risco inexistente, poucos fatores de risco) sendo a vulnerabilidade da organização também reduzida.

Classificação do impacto

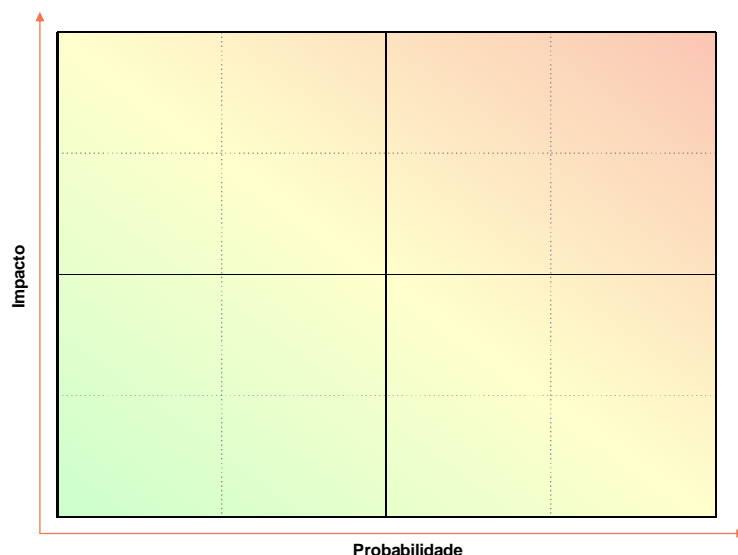
O impacto dos eventos de risco deverá ser classificado qualitativamente em termos da sua influência no alcançar dos objetivos de negócio.

A seguinte tabela define a escala qualitativa para classificação do impacto dos eventos de risco na APDL:

Classificação		Descrição
3 a 4	Muito elevado	
2 a 3	Elevado	
1 a 2	Médio	
0 a 1	Baixo	Os eventos de risco são previsíveis, de curta duração ou pontuais permitindo à organização atuar atempadamente reduzindo as suas consequências a reduzidas perdas financeiras, de imagem e reputação ou humanas.

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

O risco calculado resulta da conjugação da probabilidade de ocorrência (vulnerabilidade) com o impacto do evento de risco, e poderá ser representado graficamente numa matriz de risco cuja estrutura se apresenta a seguir:



4.4 Classificação do nível de controlo

Quanto a mitigação do risco é obtida com recurso a atividades de controlo, é necessário avaliar o nível de controlo associado a essas atividades. Esta avaliação é efetuada em duas vertentes complementares:


- **Avaliação do desenho e implementação** – Medição da atividade de controlo quanto à capacidade para prevenir, detectar e corrigir eficazmente um erro material (desenho) e se esta atividade operou pelo menos uma vez durante o período em análise (implementação); e
- **Avaliação da efectividade operacional** – Medição da atividade de controlo quanto operação contínua e eficaz durante um determinado período de tempo.

No caso de a atividade de controlo ser efectiva quanto ao desenho e implementação e não ser demonstrada a sua efetividade operacional através dos testes realizados, a conclusão é que a atividade de controlo é inefetiva.

Pelo contrário, se a conclusão sobre o desenho e implementação for de inefetividade da atividade de controlo, não fará então sentido avaliar a sua efetividade operacional concluindo-se também neste caso pela inefetividade da atividade de controlo.

Neste contexto, o nível de controlo pode ser considerado adequado ou inadequado:

- **Nível de controlo adequado** – a maior parte das atividades de controlo existentes são efetivas e não estão em falta atividades de controlo chave; e

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- **Nível de controlo inadequado** – estão em falta atividades de controlo chave ou algumas das principais atividades de controlo não são efetivas.

De referir que os níveis de controlo de determinados riscos, dada a sua natureza, não são avaliados através da efectividade de atividades de controlo, devendo ser consideradas outras ações existentes para partilhar, reduzir, evitar ou aceitar o risco.

No caso do nível de controlo ser adequado e ainda assim o nível de risco resultante ser considerado como não aceitável haverá que encontrar outras formas de lidar com o risco, como sejam partilhar o risco, aceitar o risco ou evitar o risco. Em termos de controlo interno, significa que foi encontrado um equilíbrio entre os custos e os benefícios associados à aceitação do nível de risco por parte da organização, ou seja qualquer atividade de controlo adicional traria um custo à organização superior aos benefícios para o controlo do risco.

Convém ainda referir que, apesar do nível de controlo ser classificado como inadequado, o risco pode passar para um nível aceitável face ao nível de aceitação do risco por parte da Empresa. Este facto não invalida que as atividades de controlo sejam revistas no sentido de tornar o controlo adequado, contribuindo para uma ainda maior redução do risco.


4.5 Níveis de aceitação de risco

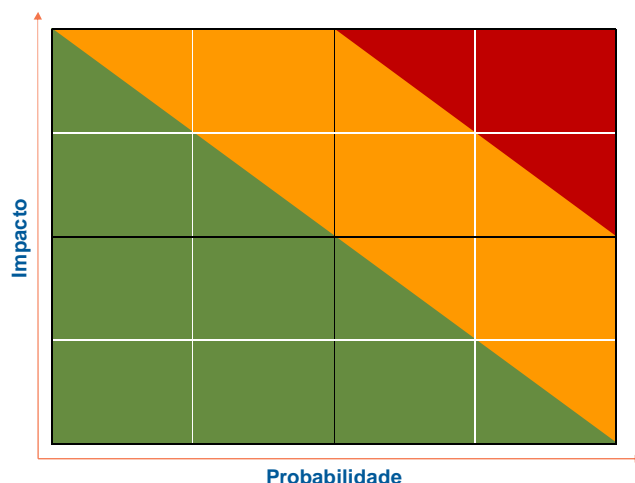
Por definição, o nível de aceitação do risco é quantidade e tipo de risco que uma organização está disposta a aceitar, alcançar ou assumir. Uma vez mais, na definição do nível de aceitação do risco deverá ser considerado o grau de maturidade do modelo de gestão do risco.

Nas primeiras iterações de aplicação do modelo de gestão do risco é natural que seja adotado um método mais simples, evoluindo este para métodos mais complexos. Os principais aspetos a considerar na definição dos níveis de aceitação do risco são:

- **Qualitativo vs. Quantitativo** – A definição de um nível de aceitação do risco qualitativo (e.g. alto, médio, baixo) encontra-se mais adaptada a um grau de maturidade onde os riscos são também avaliados de forma qualitativa; e
- **Global vs. Por risco** – A organização deverá começar por definir de um nível de aceitação do risco global, ou seja o mesmo nível de aceitação para todos os riscos evoluindo progressivamente para níveis de aceitação por categoria, por classe ou por risco.

O nível de aceitação do risco foi definido em função do risco residual, em três zonas conforme a figura abaixo:

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

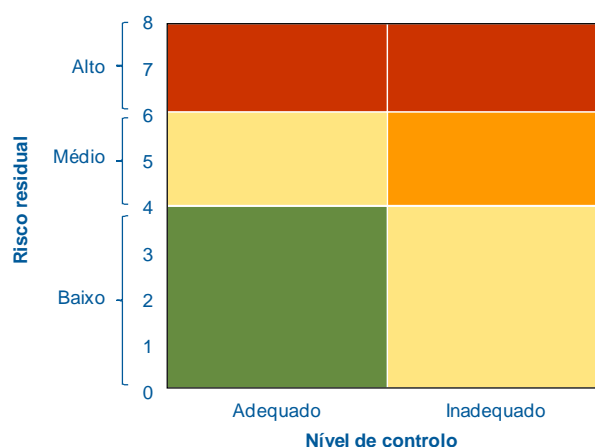



4.6 Indicadores de alerta de risco

O nível de risco residual é o resultado da efectividade das respectivas atividades de controlo, ou nível de controlo, sobre o nível de risco inerente. A tendência é que as atividades de controlo efetivas transportem o risco para uma zona de baixo risco enquanto que as atividades de controlo inefetivas não façam descer o nível de risco.

Convém, contudo, referir que o risco residual pode manter-se acima de um nível aceitável apesar do nível de controlo ser adequado e, igualmente, o risco residual pode ser aceitável apesar do nível de controlo ser inadequado. Por esta razão, as medidas a tomar para mitigação adicional do risco deverão ter em consideração não apenas o risco residual mas também o nível de controlo, como genericamente se ilustra na figura abaixo.

A seguinte figura ilustra o cruzamento do risco residual com o nível de controlo, apresentando as áreas correspondentes aos diferentes indicadores de alerta de risco (amarelo, laranja e vermelho):



	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Sempre que o risco ocupar uma das zonas de alerta, deverão ser tomadas as medidas apropriadas, de acordo com a seguinte definição:



Zona vermelha – Sempre que o risco tem um valor residual superior a 6, Independentemente do nível de controlo. São requeridas ações imediatas prioritárias para tratamento do risco. É ainda requerida a implementação de atividades de controlo adicionais ou a remediação das atividades inefetivas.



Zona laranja – Quando o risco tem um valor residual entre 4 e 6 e, adicionalmente, os respectivos controlos são inadequados. Neste caso são requeridas ações imediatas para tratamento do risco e a implementação / remediação das atividades de controlo que foram consideradas inefetivas.



Zona amarela – Esta área engloba os riscos com nível residual entre 4 e 6 apesar os controlos serem adequados, e os riscos com nível residual inferior a 4 (aceitável) mas cujos controlos são inadequados. São requeridas ações para implementação / remediação das atividades de controlo consideradas inefetivas.



Zona verde – Para os riscos cujo valor residual é inferior a 4 (aceitável) e os respetivos controlos são considerados efetivos é apenas requerida a monitorização das atividades de controlo, garantindo a manutenção do risco nesta zona.

4.7 Estratégias para tratamento de risco


A redução do risco residual para um nível aceitável é realizada através de ações de tratamento que obedecem a quatro estratégias distintas, das quais se apresentam exemplos de ações concretas:

Evitar o risco, prevenindo a exposição a eventos de risco:

- Sair de um determinado mercado ou área geográfica;
- Vender ou alienar partes do negócio;
- Abandonar atividades específicas, redefinindo objetivos, estratégias e redirecionando recursos;
- Redefinir o desenvolvimento do negócio e expandir mercado; e
- Avaliar novas alternativas de investimento.

Aceitar o risco no seu nível actual:

- Assumir o risco na sua actual forma / existência;

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

- Redefinir produtos ou serviços incluindo condições específicas que compensem o risco adicional; e
- Medidas financeiras.

Reduzir o risco, implementando medidas que baixem o risco para um nível aceitável:

- Dispersar recursos físicos, financeiros ou de informação, reduzindo o risco de perdas catastróficas inaceitáveis;
- Controlar o risco através de processos internos que reduzam a probabilidade de ocorrência de eventos de risco para um nível aceitável;
- Planear uma resposta efetiva a contingências, documentando e responsabilizando os recursos certos e promovendo a realização de testes e execução do plano periodicamente;
- Diminuir a dimensão da atividade que origina o risco;
- Melhorar características de um produto ou serviço para gerir a exposição pretendida;
- Transferir operações de uma localização onde o risco não possa ser gerido, para outra onde possa ser gerido de melhor forma;
- Redesenhar o modelo de negócio, no seu todo ou em parte; e
- Diversificar os recursos necessários para suportar o modelo de negócio da empresa.

Partilhar o risco com outras entidades independentes:


- Redefinir a estratégia de risco, contratando entidades externas para suportar parte do risco;
- Dispersar os seguros contratados, reduzindo a exposição do portfolio de seguros;
- Transferir os riscos de entrada num novo mercado através de alianças ou *joint-ventures*;
- Recorrer a *outsourcing* em processos não fundamentais do negócio, contemplando o risco e a sua partilha / gestão no contrato formalizado; e
- Partilha de risco, diretamente com entidades independentes.

4.8 Identificação de interlocutores e “donos” dos riscos

Por último, é necessário identificar os interlocutores de gestão de risco, bem como os interlocutores de cada risco.

Sendo este um processo evolutivo, os interlocutores deverão ser considerados nesta perspetiva, evitando sobrecarregar em demasia o processo no seu início e simultaneamente abranger o universo de Unidades Orgânicas incluídas no âmbito da Gestão de Risco.

Elaborado: AIQ Data: 14/07/2015	Aprovado: CA Data: 16/07/2015	Página 46 de 47
------------------------------------	----------------------------------	-----------------

	MANUAL	Código:	N/A
	GESTÃO DO RISCO EMPRESARIAL, INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS	Entrada em vigor:	16-07-2015

Os interlocutores de cada risco terão como principais responsabilidades:

- Conhecer em pormenor os aspetos relacionados com o risco, nomeadamente risco inerente, medidas de mitigação em vigor, risco residual, planos de tratamento;
- Assegurar que as medidas identificadas e previstas para cada risco desempenham a sua função corretamente, ou seja que se encontram desenhadas, implementadas e a operar com eficácia; e
- Interagir com os interlocutores de gestão do risco, nomeadamente alertando para situações anómalas ou aspetos que possam ser relevantes para o processo de gestão de risco do Grupo.

Em anexo é apresentada uma lista dos interlocutores identificados no processo de gestão do risco e uma lista interlocutores de cada risco.