Gestão de dados de Risco

Um caso de um registo de risco desenvolvido em tecnologia Outsystems

Diogo Miguel Galhardas Pinto Gonçalves

Dissertação para obtenção de Grau de Mestre em

Engenharia Informática e de Computadores

Orientador: Prof. José Luís Brinquete Borbinha

Jurí

Presidente: Prof. Luís Manuel Antunes Veiga

Orientador: Prof. José Luís Brinquete Borbinha

Vogal: Prof. Sérgio Luís Proença Duarte Guerreiro

Outubro 2019

Agradecimentos

Gostaria de mostrar a minha gratidão ao meu orientador, professor José Borbinha, e ao CRO (Chief Risk Officer) da INCM (Imprensa Nacional da Casa da Moeda), Ricardo Viera, pelo apoio e orientação nesta tese. Certamente que o profundo conhecimento e a experiência que têm, contribui para desenvolver a minha pesquisa e obter um trabalho mais consolidado. Gostaria também de a todos os membros que na INCM contribuíram para que o meu trabalho chegasse ao fim e o mais perto possível de uma boa ferramenta.

Também sou muito grato a todos os meus amigos mais próximos, eles que estiveram sempre presentes e sempre me apoiaram ao longo deste percurso, e com eles partilhei alguns dos momentos mais importantes nos meus anos de Universidade.

Por último, as minhas maiores palavras de gratidão vão para toda a minha família, que sempre mostraram interesse nos meus sucessos académicos e sempre me apoiaram, principalmente aos meus pais e a minha irmã que sempre me aconselharam da melhor forma durante estes anos todos, e também à Rita, pelo o amor e amizade incondicional.

Resumo

Gestão de risco nos últimos tempos tornou-se um conceito para vez mais vantajoso aos olhos das organizações, e por esse motivo, estas mesmas organizações tentam desenvolver estratégias de gestão de risco. As estratégias de gestão de risco consistem no processo de reconhecer, observar e eliminar as ameaças da organização, e adicionalmente, uma estrutura para suportar este processo. A estrutura necessária para suportar resultará numa estrutura de gestão de risco geralmente conhecida como "*risk register*" ou "registo de riscos".

A aplicação que será desenvolver neste projeto irá ser feita com a tecnologia OutSystems e tem com base algumas ferramentas já existentes, tendo como objetivo suportar uma estrutura de gestão de risco respondendo assim às necessidades específicas do caso de estudo da *Imprensa Nacional Casa da Moeda* (INCM).

A organização deste caso de estudo (INCM) é portuguesa e é responsável por várias operações de serviços de Estado Português, como por exemplo, cunhagem da moeda metálica, produção do cartão de cidadão e passaporte, entre outras operações.

Palavras Chave

Risco, Gestão de Risco, INCM, OutSytems, gestão do risco corporativo

Abstract

Risk management in recent times has become an increasingly advantageous concept in the eyes of organizations, and for this reason, these same organizations are trying to develop risk management strategies. Risk management strategies consist of the process of recognizing, observing and eliminating threats from the organization, and additionally a framework to support this process. The structure required to support will result in a risk management framework commonly known as a risk register.

The application that will be developed in this project will be made with OutSystems technology and is based on some existing tools, aiming to support a risk management structure, thus meeting the specific needs of the case study of the National Press House (INCM).

The organization of this case study (INCM) is Portuguese and is responsible for various Portuguese State service operations, such as coinage, citizen card production and passport, among other operations.

Keywords

Risk, risk management, INCM, OutSytems, enterprise risk management

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

AICPA	American Institute of Certified Public Accoutants
BPMN	Business Process Model and Notation
CRO	Chief Risk Officer
CGRC	Comité de Gestão de Riscos Corporativos
DSRM	Design Science Research Methodology
DSDM	Método Dinâmico de Desenvolvimento de Sistemas
ERM	Enterprise Risk Management
FERMA	Federation of European Risk Management Associations
ISO	International Organization for Standardization
INCM	Imprensa Nacional-Casa da Moeda
TI	Tecnologias de Informação
UC	Use Case
UML	Unified Modeling Languge

1

1. Introdução

O contexto da Gestão de Risco na INCM é caracterizado na atualidade pela existência de várias Estruturas de Gestão de Risco Especializadas, cada uma focada em dar respostas concretas a necessidades operacionais (por exemplo, para obtenção de certificações) ou de negócio (por exemplo, para resposta a concursos nacionais e internacionais). Deste modo, a Estrutura de Gestão de Riscos Corporativos deverá visar ter como objetivo o desenvolvimento de uma ferramenta que, tirando vantagem das Estruturas de Gestão de Risco Especializadas já existentes, deverá permitir oferecer num dado momento uma visão comum e transversal dos riscos operacionais e de negócio da organização.

Para satisfazer esses objetivos é necessário resolver uma contradição: por um lado que a organização adote conceitos e princípios de gestão de risco comuns, enquanto por outro lado tal não pode constringir a definição de Processos de Gestão de Risco Especializados para os diversos contextos de negócio da organização. Esta contradição pode, no entanto, ser aparente se for conseguido desenhar e pôr em prática uma infraestrutura para uso comum, isto é, de uma solução tecnológica para gestão de um Registo de Riscos e com capacidade de geração de Relatórios de Risco, que sirva ao mesmo tempo cada contexto especializado e o objetivo da Gestão de Risco Corporativo. Isto é, uma infraestrutura que possa gerir toda a informação de risco de forma uniforme e transparente para as partes interessadas em cada um dos contextos, ao mesmo tempo que lhes garante serviços de suporte às suas atividades do Processo de Gestão de Risco, incluindo Relatórios de Risco, segundo as reais necessidades do respetivo contexto.

Para suportar a implementação do Processo de Gestão de Risco e o modelo de domínio comum à organização é necessário definir uma adequada infraestrutura de suporte. A Gestão de Risco Corporativo na INCM será suportada por um sistema de informação que irá suportar a definição e integração de Registo de Riscos. Um Registo de Riscos é um objeto onde a informação de risco é registada. Mais concretamente, é uma ferramenta de suporte considerada essencial para a comunicação, consulta, monitorização e revisão dos riscos – os principais objetivos da gestão de risco corporativo.

O Registo de Riscos é também a base para a integração da informação. Através dos diversos registos de Riscos criados pelos diferentes processos de Gestão de Risco, o sistema de informação a implementar deve permitir a agregação de toda a informação num Registo de Risco Corporativo. De maneira a possibilitar tal agregação é necessário que todos os registos de riscos criados tenham, pelo menos, os conceitos definidos para o registo corporativo. É importante referir que tipicamente a governação de risco apenas tem preocupações com riscos que ponham em causa o funcionamento da organização. É, portanto, necessário que a agregação permita também filtrar a informação de risco com base nas preocupações das partes interessadas, o que pode ser obtido através do estabelecimento do contexto por objetivos. Ou seja, deve ser concebido um Registo de Riscos de tal forma que possam ser listados e analisados Riscos relevantes para apenas um ou mais objetivos determinados.

1.1. Descrição do problema

O problema existe quando as organizações, neste caso INCM, têm a necessidade de usar ferramentas que auxiliem nesta gestão.

No caso concreto na INCM, que aborda uma estratégia de gestão de risco, necessita de ferramentas auxiliares. Atualmente utiliza um Excel com uma série de procedimentos como auxílio, no entanto esta prática para além de não ser exímia, não é intuitiva de usar.

Com o objetivo de auxiliar a INCM, o INESC começou por desenvolver uma ferramenta chamada HoliRisk, no entanto devido às constantes mudanças de requisitos tornou-se difícil finalizar, em desenvolvimento ágil, a ferramenta de maneira a que a INCM conseguisse utilizar durante a gestão de risco.

Portanto é necessário desenhar, concretizar, demonstrar e validar um registo de risco tendo em conta os requisitos usados pela INCM.

1.2. Objetivos do trabalho

O objetivo deste trabalho passou por recolher todos os requisitos e especificações necessárias para desenvolver uma aplicação de "registo de risco" utilizando a tecnologia OutSystems, que consiga suportar a gestão de risco.

Os requisitos que serão usados para o desenvolvimento de uma ferramenta de gestão de risco correspondem aos requisitos funcionais da INCM em Apêndice A, por motivos de confidencialidade não foi possível usar os dados da INCM, no entanto foi fornecido um caso artificial da pizaria, que se assemelha à INCM, para demonstração da solução.

1.3. Método de desenvolvimento

Utilizando a *design science research methodology* (DSRM) [44], o problema foi identificado seguindo-se a descrição da motivação para o mesmo. Esta ação inclui a identificação da bibliografia relevante para o tema assim com a compreensão da importância da solução parra o problema. O passo seguinte passo por definir os objetivos da solução, para que de seguida fosse possível desenhar e desenvolver uma solução que fosse de encontro com os objetivos estabelecidos inicialmente. Como isto resultou na criação de um artefacto que foi avaliado através de um caso de estudo, observando e medindo quão eficaz e eficiente era a solução para o problema.

A criação do artefacto que nesta dissertação se refere à aplicação desenvolvida em OutSystems para a INCM decorreu num processo gradual e demorado de construção e avaliação. Cada ciclo de desenvolvimento foi alvo de revisão através de reuniões realizadas com CRO da INCM e com o orientador da dissertação.

1.4. Estrutura do documento

Este documento está estruturado da forma que se descreve de seguida.

Na secção 2 é dado algum contexto teórico sobre risco, são apresentados os conceitos fundamentais da gestão de risco, e de seguido é explicado todo o processo da gestão de risco.

Na secção Tecnologia e Método de Desenvolvimento, é apresentada a tecnologia OutSystems, como trabalho relacionado do projeto. Neste capítulo é feita uma visão geral ao conceito da aplicação e benefícios em usar esta ferramenta de desenvolvimento

ágil. Ainda nesta secção é apresentado o método que se usou para o desenvolvimento da aplicação, que corresponde ao método usado no desenvolvimento com a tecnologia OutSystems.

Análise do Problema dedica-se à análise do problema, contextualizando o estado atual da INCM.

De seguida na Análise do Modelo de Domínio é apresentado o modelo de domínio onde se baseia o desenvolvimento da aplicação.

Na Análise dos requisitos e desenho do caso de motivação, são apresentados os requisitos que foram desenvolvidos durante a dissertação, assim como os casos de uso que resultam destes mesmos requisitos. Por fim é apresentado o desenvolvimento feito nesta dissertação.

Com secção Demonstração da solução, é apresentado o caso artificial fornecido pela a INCM de forma a validar a aplicação desenvolvida com dados que sejam possível testar como se fossem os da INCM, visto que por motivos de confidencialidade não foi possível usar dados da INCM.

Na última secção finaliza com as conclusões finais sobre o trabalho realizado bem como são apresentadas ideias para dar seguimento a presente dissertação.

2

2. Enquadramento teórico

Nesta secção é descrito os principais conceitos sobre gestão de risco, para uma melhor compreensão do problema.

Gestão de risco são as “atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco” [18], ou seja, corresponde a um processo cíclico de gestão onde o objetivo passa por identificar, analisar e mitigar os riscos que possa interferir que possa interferir com os objetivos e operações da organização

2.1 Fundamentos da Gestão de Risco

A arte da gestão de riscos é essencialmente identificar os riscos específicos de uma organização e responder de forma apropriada. A gestão de riscos é um processo formal que permite a identificação, avaliação, planeamento e gestão de riscos.

Todos os níveis de uma organização precisam de ser incluídos na gestão de risco para que esta seja eficaz. Estes níveis são geralmente designados por corporativos (definição de políticas), negócios estratégicos (linhas de negócios) e projeto.

É referido que em [1] a origem da palavra “risco” é considerada através da palavra árabe “risq” que significa “tudo o que foi dado a si (por Deus) desenha lucro e tem conotações de um resultado fortuito e favorável” ou a palavra latina “riscum” que originalmente referia-se ao desafio e tinha conotações de evento fortuito, mas desfavorável.

A proposta a definição de risco dade em [2]: "O potencial para consequências negativas indesejáveis de um evento ou atividade", enquanto muitos autores definem risco como "a medida da probabilidade e da gravidade dos efeitos adversos”.

A gestão de riscos necessita de levar em consideração a interação destes níveis e refletir os processos que permitem comunicar e aprender uns com os outros. Merna e Merna [3] acreditam que os riscos identificados em cada nível dependem das informações disponíveis no momento da avaliação, com cada risco avaliado com mais detalhes, è medida que mais informações se tornam disponíveis. O impacto do risco está relacionado com o tempo. A figura seguinte ilustra os possíveis resultados do risco.

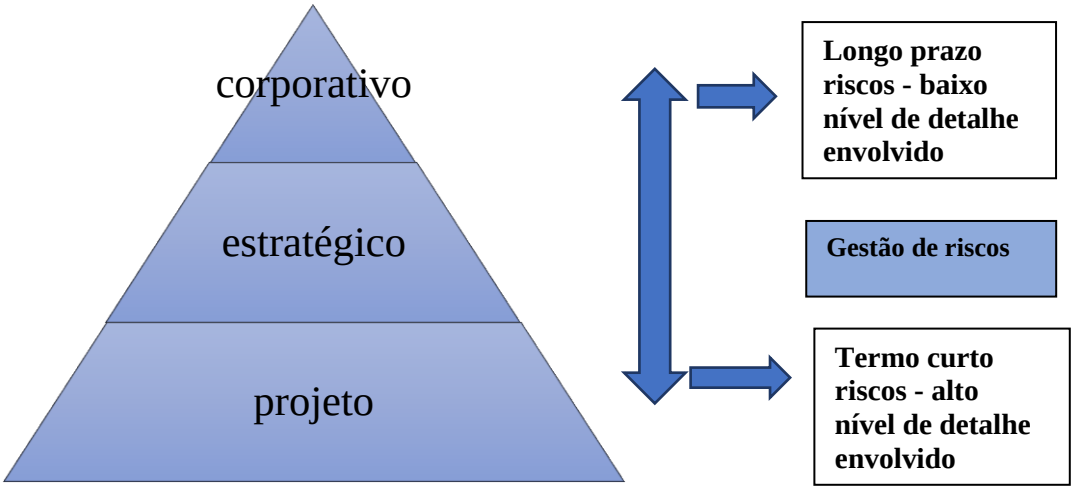


Figura 1- possíveis resultados do risco.

O modelo de Flanagan e Norman [3] sugere que o risco é composto de quatro parâmetros, a probabilidade de ocorrência, gravidade do impacto, suscetibilidade a mudanças e o grau de interdependência com outros fatores de riscos. Este modelo pode ser utilizado para descrever situações de risco ou eventos de quaisquer investimentos para a análise de risco.

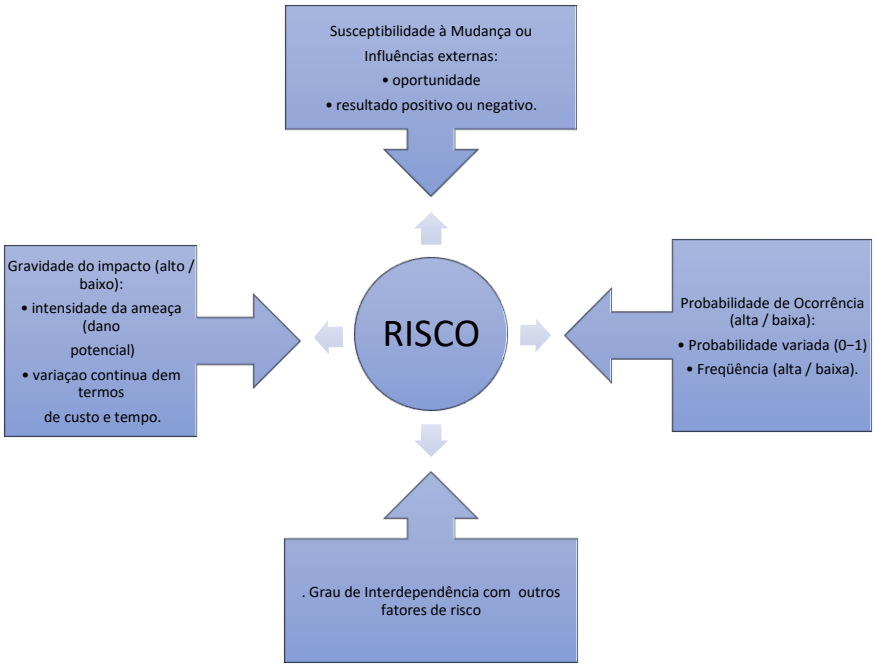


Figura 2 - Modelo de Flanagan e Norman, quatro parâmetros

Para reforçar o uso comum, interoperável e sistemático das abordagens à gestão de riscos deve ser utilizada uma gestão de risco padronizada. Esta abordagem, promove a comparabilidade e uma partilha da compreensão das informações e análises no processo

de tomada de decisão informada. O risco de segurança interna é um processo de gestão que deve ser implementado com base no risco anteriormente articulado e nos princípios de gestão [5]. A base para cada elemento do processo de gestão de riscos é a comunicação eficaz com as partes interessadas, parceiros e clientes. A comunicação bidirecional e consistente ao longo do processo ajuda a garantir que o tomador de decisões, os analistas e os responsáveis por implementar qualquer decisão partilhem um entendimento comum sobre o que é o risco e quais os fatores que podem contribuir para a sua gestão. Os conceitos como a incerteza, perceção e tolerância à perda que estão interligados com o conceito de risco, devem ser contabilizados como parte desta comunicação [5].

Para executar a gestão de risco é fundamental definir o contexto para a decisão. Para a solução complexa de problemas, a organização normalmente coloca uma equipa de gestão para auxiliar os tomadores de decisão a passar pelo processo de gestão de riscos. Ao definir o contexto informará e moldará os estágios sucessivos do ciclo de gestão de riscos.

A gestão de riscos pode ser implementada também na abordagem ágil, que avalia subsequentemente a forma de gerir todos os riscos. Se lidarmos com os riscos durante o período de desenvolvimento, criaremos as melhores condições para reações apropriadas e efetivas aos riscos. Frequentemente até um membro da equipa não precisa saber sobre uma possível existência e solução dos riscos independentes antes da fase de desenvolvimento do produto. A partir deste ponto de vista, a gestão implícita de riscos deve ser uma ameaça menor para uma solução de risco ineficaz.

Muitos projetos falham devido ao baixo nível de maturidade do projeto. A implementação de uma metodologia ágil de gestão de riscos é uma das principais tendências do processo de desenvolvimento de software de reestruturação [6].

As metodologias ágeis tentam definir algumas áreas como o ciclo de vida do projeto, gestão de equipa, engenharia e entrega. Nem todos os métodos cobrem estas aéreas. Como exemplo, o DSDM descreve todas as áreas, mas apenas a gestão do projeto da equipa de Scrum do ciclo de vida [6].

O foco na gestão de equipas e a sua importância está em todas as metodologias ágeis. Sem uma equipa de projeto eficaz e auto-organizada, composta por indivíduos capacitados e motivados a implementação esta metodologia tem sido contestada. Outros fatores de sucesso do desenvolvimento ágil de software têm sido relacionados com os fatores organizacionais, pessoas, processos, técnicos e projetos [7].

De uma forma geral, a implementação desta metodologia inclui a identificação da metodologia apropriada, identificação de requisitos específicos da empresa, adaptação e implementação da metodologia. A adaptação da metodologia ágil tem sido analisada com diferentes focos, as abordagens que podem ser usadas para a adaptação da metodologia ágil variam de ágil específico, desenvolvimento de software específico aos métodos gerais de engenharia [8].

A adaptação é efetuada através da identificação de papéis, práticas, artefactos e processos que precisam de ser adequados para a situação atual. A situação é identificada com diferentes fatores relacionados com a equipa, interna e externa, objetivos, níveis de maturidade e conhecimentos prévios [9].

Por outro lado, o princípio da precaução fornece a orientação sobre como lidar com os riscos. Não é uma regra de decisão, interpretada num sentido restrito, que inclui uma observação para uma ação. O que se enfrenta são possíveis observações, eventos e os seus efeitos. Formaliza-se o cenário estudado considerando uma atividade interpretada num sentido amplo, por exemplo, um investimento ou a vida de um país. Esta atividade pode conduzir a algumas consequências quando se observa o futuro e, está sujeito a incertezas. E, são estas incertezas que nos leva a teorias como a teoria da utilidade subjetiva esperada, que compara as opções através do uso do utilitário esperado [10].

A atividade de gestão de risco inclui o fornecimento de executivos e pessoal em diferentes níveis de organização com recursos contínuos, relevantes e informações confiáveis, projetando estruturas e sistemas práticos para estabelecer as decisões de gestão de risco. No entanto o objetivo da gestão de riscos não se limita apenas a minimizar os riscos e as situações de risco, mas sim ter em mente que os negócios estão sempre associados a exposições, e o objetivo principal de uma gestão eficaz de riscos é manter o equilíbrio entre o risco e o retorno [11].

Diadagra (2013) desenvolveu um modelo para investigar a relação entre a gestão de risco e o sucesso de projetos de tecnologias e, este modelo consistia na gestão de risco em quatro categorias, identificação de riscos, análise de riscos, planeamento de respostas a riscos e monitorização e controlo de riscos. Os resultados do estudo determinaram que a identificação de riscos e o planeamento de riscos não influenciaram o desempenho subjetivo do projeto em termos de confiabilidade, facilidade, flexibilidade, satisfação e qualidade. Neste caso, as conclusões não puderam ser generalizadas para todas as empresas de TI devido ao reduzido tamanho da amostra para uma margem de erro inaceitável.

Crader [12] referiu que todo o projeto tinha risco por exemplo; os recursos deixaram a organização, a liderança mudou e os orçamentos foram cortados etc., muitos fatores além do controlo. No entanto, muitos riscos para projetos podem ser reduzidos ou mesmo eliminados com a previsão e gestão contínua.

De salientar que o sucesso dos projetos de tecnologias de informação, é uma área de preocupação para muitas organizações em todo o mundo. Existe uma variedade de abordagens sobre a medição do sucesso do projeto. Neste contexto, DeLone e McLean [13] expressaram 6 medidas para a informação do sucesso de projeto do sistema: qualidade do sistema, satisfação do usuário, qualidade da informação, uso da informação, impacto organizacional e impacto individual.

Muitos autores sugeriram que os projetos deveriam ser classificados como bem-sucedidos quando são concluídos dentro do cronograma e do orçamento estimados e produzem um nível aceitável de desempenho [14].

Mahaney e Lederer [15] realizaram um estudo utilizando um projeto concluído dentro do prazo e dentro do roçamento que funcionou como as medidas para avaliação do sucesso do projeto.

Segundo Baccarini [16] o sucesso do projeto envolve dois componentes, como o sucesso da gestão de projetos e o sucesso do produto. O desempenho é o grau em que o projeto de software alcança o sucesso na perspetiva de processo e do produto.

O estudo de Daranee & Veera [17] teve como objetivo explorar as práticas de gestão de risco que influenciam o sucesso de projetos de TI. Os dados foram colhidos de 200

gestores de projetos, analistas de TI nas empresas. Os resultados demonstraram que as diferenças nos tipos organizacionais afetaram o sucesso dos projetos de TI em todos os aspetos, enquanto as diferenças nos tamanhos organizacionais afetaram o sucesso dos projetos de TI em termos do aspeto do desempenho do produto, bem como de outros aspetos.

2.2 ISO 31000

De acordo com a Norma ISO 31000 [18], a finalidade da gestão de riscos é a criação da proteção de valor, a qual melhora o desempenho, estimula a inovação e suporta a consecução de objetivos definidos pela organização. Esta Norma, engloba todos os tipos de riscos em qualquer contexto e, é construída com base em três pilares, os princípios de gestão de riscos, guia da gestão de riscos e o processo de gestão de riscos.

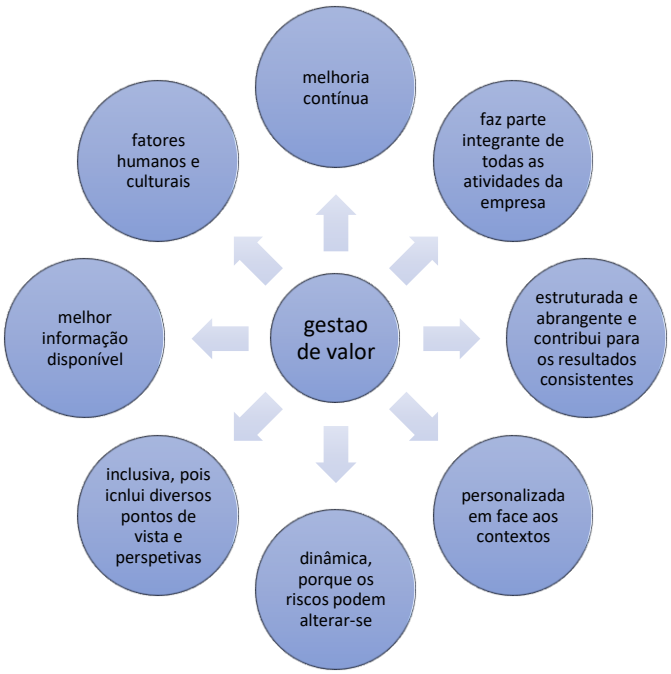


Figura 3 - Princípios da Norma ISO 31000

"*Na sociedade contemporânea pretende-se com estes princípios, divulgar na organização, como pontapé de saída da implementação, que as incertezas e os riscos são preocupações dominantes no contexto empresarial, assim como na gestão de qualquer empresa, no caso de bens públicos*", de acordo com Almeida [19].

Importa referir que no ano de 2009, o organismo ISO publicou a norma internacional ISO 31000 que é aplicável à gestão de todas as formas de risco em qualquer contexto industrial [20].

A ISO 31000, em comparação com as principais normas de gestão de risco, tem um papel de destaque em decorrência ao reconhecimento internacional do organismo ISO. A estrutura desta Norma é constituída por [20]:

a) Vocabulário;

b) Conjunto de critérios de desempenho;

c) Processo abrangente comum para a identificação, análise, avaliação e tratamento de riscos;

d) Guia de como o processo de gestão de risco pode ser integrado ao processo de tomada de decisão de qualquer organização.

De acordo com a norma ISO 31000 a definição de risco altera a preocupação de algo ocorrer pela probabilidade de um efeito nos objetivos, ou seja, gerir os riscos representa um processo de otimização que estimula o alcance do objetivo principal, e assume que o risco é quotidiano, não sendo considerado bom nem mau [20]. Dito de outra forma, a gestão de riscos associa-se aos aspetos positivos e negativos das atividades, e procura maximizar o primeiro e anular ou reduzir o segundo.

Importa ainda salientar que a ISO 31000 é composta de um conjunto de opções genéricas que devem ser consideradas enquanto um risco é tratado, tais como:

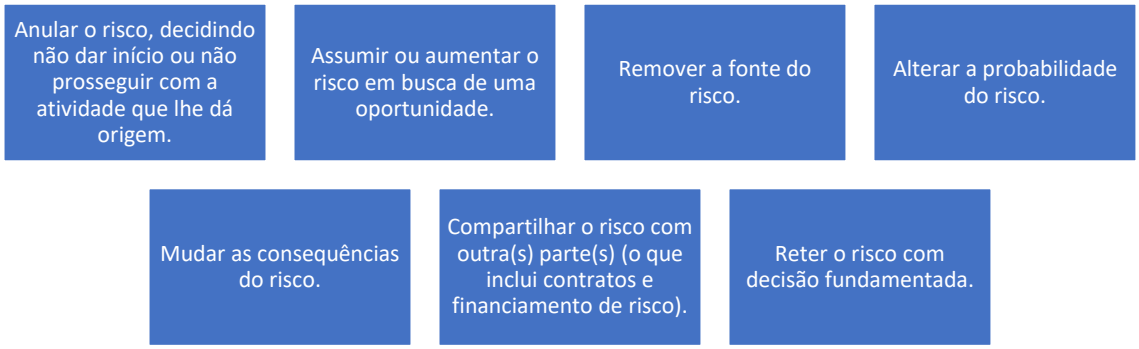


Figura 4 - Opções da Norma ISO 31000

De acordo com Aven a avaliação de risco faz parte de um domínio distinto da "tomada de decisão" [10], ou seja, a primeira atividade é a base para a segunda, e não prescreve somente como o risco deve ser tratado

O objetivo principal da gestão de riscos é auxiliar a empresa na integração da gestão de riscos em qualquer uma das suas atividades e funções. A sua eficácia irá depender da sua integração no processo de governação da organização, mesmo no processo de tomada de decisão. Assim, o desenvolvimento da estrutura inclui o design, implementação, avaliação, e melhoria da gestão de riscos em toda a organização, através da liderança e compromisso

Figura 5 - Estrutura da gestão de riscos

É assim, exigido através da Norma ISO 31000 que exista um compromisso forte e sustentado da gestão de topo e, que unifique num propósito a implementar. A gestão de riscos impõe, desta forma um compromisso mandatário sustentado, tornando possível o envolvimento de todos e em todas as áreas da empresa.

Qualquer organização gere o risco de acordo com a sua própria identificação e análise, após a avaliação da necessidade da sua alteração, e com o objetivo de satisfazer todos os critérios de risco. Assim, no decorrer deste processo, é importante a comunicação entre todas as partes, ao mesmo tempo que se monitoriza e revê o risco e os meios de controlo que os estão a influenciar, garantindo sempre a melhoria contínua.

Dito de outra forma, um sistema de gestão de riscos corresponde a um conjunto de medidas e controlos de atuação organizacionais que sejam capazes de inimizar as incertezas, a um nível aceitável de forma a atingir a maximização do lucro

Seguindo esta linha de pensamento é possível dividir as atividades de gestão de riscos em 3 fases como é descrito pela ISO 31000,

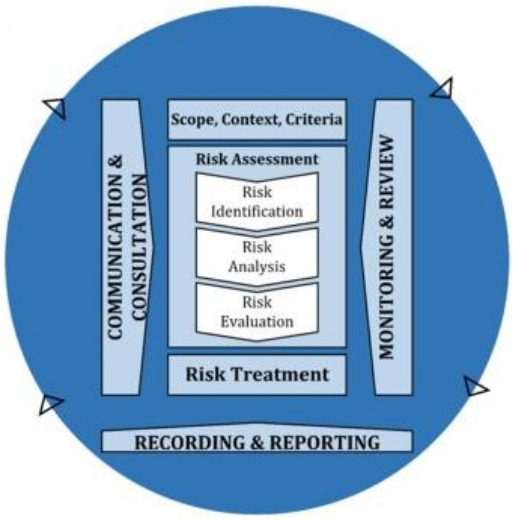


Figura 6 - Processo da gestão de risco

A primeira atividade consiste no **estabelecimento do contexto** e envolve a compreensão de fatores externos relacionados com as atividades realizadas pela organização para tentara atingir os seus objetivos e fatores relacionados com o ambiente interno da própria organização. Visto que todas as organizações diferem umas das outras, o processo da gestão de risco deve ser adaptado [18]. Nesta fase também é definido os critérios de risco da organização, que inclui o nível de cada risco, o impacto associado a cada um, e nível ao qual o risco pode ser aceite. Mesmo sendo os critérios dos riscos serem definidos no início do processo, "eles são dinâmicos e deverão ser continuamente revistos e, se necessário, modificados",[18].

A segunda atividade corresponde à **apreciação dos risco,** onde o objetivo passa por identificar o risco, analisá-lo e por fim avaliar se é possível avançar para o tratamento do mesmo ou não. Seguindo esta linha de pensamento é possível dividir esta atividade em 3 fases como é descrito pela ISO 31000, [18]:

•Identificação dos riscos, nesta fase, após o contexto ter sido estabelecido, é criada uma lista onde são identificados todos os riscos. Cada risco é descrito de acordo com uma causa, evento e consequência e deve ser associado a um dono, que será responsável pela gestão do risco. Neste processo qualquer evento que traga impacto nos objetivos da organização, sejam positivos ou negativos, é tendo em conta para a seleção dos riscos, por isso neste processo é importante seja dada importância ao fator humano para a identificação dos riscos

•Análise do risco, sobre a lista de riscos identificados no passo anterior, e utiliza toda a informação recolhida, de modo a determinar qual a verossimilhança das consequências, qual o seu impacto e a combinação dos dois, para saber qual o nível do risco. Se existirem controlos para certos riscos, também devem ser considerados nesta análise. Nesta análise é possível classificar a verossimilhança e o impacto de uma forma quantitativa e/ou de uma forma qualitativa. Qualitativa corresponde a separar a escala por categorias (Muito Alta, Alta, Média, Baixa, Muito Baixa), e quantitativa consiste em dividir a escala por valores numéricos (1,2,3,4,5), como está representado na **Figura 7**. Nesta fase pode existir a dificuldade de analisar riscos com incerteza elevada e "isto pode ser um problema ao analisar eventos com consequências severas", e nestes casos torna-se evidente a necessidade de utilização de técnicas para facilitar esta análise.

Score	Impact	Likelihood	Consequence(euro)
5	Very High	The event is estimated to occur once a month	More than 40.000 (huge loss)
4	High	The event is estimated to occur once every 2 to 5 months	15.000 to 40.000 (high loss)
3	Medium	The event is estimated to occur once a year	5.000 to 15.000 (medium loss)
2	Low	The event is estimated to occur once every 3 to 6 years	1.000 to 5.000 (some loss)
1	Very Low	The event is estimated to occur once every 10 to 20 years	Less than 1.000 (minimal loss)

Figura 7 - Exemplo de uma escala quantitativa e qualitativa

•Avaliação do risco, por fim nesta fase avalia-se dos resultados da fase anterior com o objetivo de apoiar na tomada de decisões. Envolve uma avaliação sobre o nível do risco segundo os critérios de risco da organização, de modo a perceber melhor quais são os riscos que devem ser tratados ou se os controlos que existem param um certo risco são suficientes. Deste modo é possível definir por que ordem os riscos devem ser tratados,

dependendo a sua gravidade. “O resultado da avaliação dos ricos deverá ser registado, comunicado e depois validado nos níveis apropriados da organização”[18].

Por último, a terceira atividade do processo de gestão de risco, é o **Tratamento do risco.** Nesta atividade consiste num processo iterativo. Começa-se por formular e escolher as opções de tratamento, de seguida planeasse a implementação do tratamento do risco. Verificar qual é a eficácia do tratamento escolhido e com isto decidir se o risco residual é aceitável, se não for deve-se fazer um tratamento suplementar. O tratamento do risco pode ter vários tipos de ações: aceitar ou aumentar o risco de maneira a explorar uma possível oportunidade; evitar o risco, parando as atividades ou os processos relacionados com as suas causas; a verossimilhança do risco e os impactos podem ser minimizados através dos controlos. No final da atividade todos os decisores e partes interessadas devem estar informadas sobre o risco residual, que “deverá ser documentado e sujeito a monotorização, revisão e, quando apropriado, tratamento suplementar”, [18].

Durante estas três atividades, existem outras três atividades que ocorrem em simultâneo com o decorrer de todo o processo da gestão de risco.

Comunicação e consulta, é uma dessas atividades, tem como objetivo ajudar as partes interessadas a terem uma melhor perceção do risco, ou seja, a comunicação procura consciencializar a compreensão do risco, enquanto a consulta envolve a obtenção de informação para ajudar na tomada de decisões. Toda esta atividade com as partes interessadas deverá ser “integrada em todas as etapas do processo da gestão de risco, [18]. Esta atividade resulta de nem todas as partes interessadas partilharem o mesmo ponto de vista.

Todos os processos devem ser controlados, monitorizados e revistos regularmente, de modo a manter toda a informação, relativa ao processo da gestão de risco, precisa e atualizada. Nesta atividade de **monitorização e revisão,** para além de ter que ocorrer em todas as fases do projeto, os seus resultados devem ser “incorporados nas atividades de gestão de desempenho da organização, de medição e de reporte”, [18].

Neste seguimento, surge a última destas três atividades, **Registo e Reporte,** onde ficam documentados os resultados do processo da gestão de risco. Esta atividade, visa

comunicar as atividades e resultados, fornecer informações para a tomada de decisões, apoiar as iterações com as partes interessadas e com isto melhorar as atividades da gestão de risco, [18].

2.3 Gestão de Risco num Contexto Empresarial (ERM)

A gestão de risco representa uma função corporativa relativamente, recente. Os principais marcos históricos foram uteis, no sentido de ilustrar a sua própria evolução ao nível empresarial. A gestão de riscos moderna, iniciou-se depois de 1955. Desde o início dos anos 1970, o conceito de gestão de risco financeiro evoluiu de forma considerável, tornou-se uma importante ferramenta de proteção concorrente que complementa várias outras atividades de gestão de risco. Após a Segunda Guerra Mundial, grandes empresas com ativos físicos elevados, iniciaram o desenvolvimento de seguros contra os riscos.

A norma ISO 31000 [18] define risco como sendo o efeito da incerteza sobre os objetivos desenhados pela organização.

Segundo a FERMA[1] o "risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências".

A gestão de risco apresenta um amplo campo de aplicação, desde produtos, serviços, processos, pessoas, bens materiais, bens sociais e ambientais, até as próprias atividades das organizações. Igualmente, a escala de riscos constitui uma característica distinta e que limita a escolha das técnicas e metodologias de identificação, análise e avaliação de riscos empresariais.

A evolução ao nível regulamentar e legislativo do setor empresarial, bem como a evolução da concorrência, conduzem a uma necessidade cada vez maior de uma gestão de riscos eficiente. São aspetos como a quebra da governação a uma escala global, o crescimento insustentável da população mundial, as disparidades económicas e sociais em zonas geográficas diferentes, suportam a estrutura económica e social atual, e são riscos de devem assumir uma importância crescente nas empresas.

[1] FERMA (2003)– Federation of European Risk Management Associations, agrega as principais organizações de gestão de riscos do Reino Unido - The Institute of Risk. https://www.ferma.eu/

São riscos que foram identificados pelo World Economic Forum [21] aos quais podem ser agrupados em subcategorias, principalmente, nas falhas do sistemas financeiro, disparidade de rendimentos, sendo crucial, a gestão eficaz destes risco para a sustentabilidade de setores da economia. De uma forma geral, o desafio das empresas está relacionado com a definição de parâmetros em que se rege a gestão de risco e efetuar uma implementação efetiva do processo. É, pois, importante que a empresa possa avaliar os riscos da sua área de concorrência, em associação com o risco fiscal.

O *American Institute of Certified Public Accoutants* (AICPA) recomenda classificar os riscos em três Grupos:

•Riscos relacionados com o ambiente empresarial que estão relacionados com as ameaças do ambiente empresarial em que a entidade atua, como os riscos decorrentes de atuação.

•Riscos relacionados com o processo de negócio e dos seus ativos, como as ameaçam ao negócio da organização pelos concorrentes e perdas de ativos.

•Riscos relacionados com a informação através da ocorrência de ameaças decorrentes de má qualidade de informações param o processo de tomada de decisão e disponibilidade de informação a terceiros.

Correr riscos faz parte da realidade empresarial, a performance depende, deste modo, da boa gestão de riscos de forma a minimizá-los ou transformá-los em oportunidades, no sentido de criar valor para a empresa. A perda de uma oportunidade pode implicar o surgimento de um risco e indicar uma redução de valor para a empresa.

Segundo FERMA o “risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências”.

A avaliação, gestão e partilha de risco representa uma das principais características do setor bancário. Numa comparação com os mercados financeiros, os bancos lidam melhor com os riscos [22]. Embora esta capacidade seja evidente, a posterior materialização durante a crise levantou algumas dúvidas em termos de enfrentarem os incentivos adequados para gerir eficazmente o risco em nome dos depositantes e investidores [23].

Com o decorrer dos últimos 25 anos, houve um elevado processo de liberalização do setor bancário em vários países. Desenvolvimento que alterou os incentivos para assumir riscos em quase todo o setor bancário. Com a globalização dos mercados financeiros, a desregulamentação teve como principal finalidade obter ganhos económicos em torno de uma maior concorrência. Os resultados demonstraram uma diminuição da regulamentação sobre restrições no setor bancário e, por consequência, um aumento da concorrência. Nos EUA por exemplo, esta forte liberalização desmantelou as barreiras para a expansão geográfica do setor bancário e incluiu uma desregulamentação de longo alcance das atividades de investimento [24].

Tendo em conta estes pressupostos, refere-se que as respostas regulamentares a estes novos incentivos para adquirir novos riscos, a nível global, concentraram-se nas recomendações de Basileia, no capital próprio como pedra angular da regulamentação prudencial.

A evidência empírica ao nível da diversificação do risco no sistema bancário nos EUA e no resto dos países da Europa é bastante diversa [25]. Os resultados destes estudos demonstram a crescente dependência das receitas não financeiras, as quais não foram associadas com a volatilidade reduzida dos lucros, ou da diminuição sistemática de risco, associada aos retornos de mercado de ações.

Em maior parte das especificações empíricas existe um conjunto de variáveis que concorrem para os principais fatores macroeconómicos e institucionais, nomeadamente, a evolução da habitação e mercados patrimoniais, concorrência e governança corporativa.

No entanto, o que se afirmou – e se repete – que o impacto da concorrência sobre o risco bancário é ambíguo, isto porque, a maior concorrência pode conduzir a uma maior assunção de riscos por parte dos bancos [26]. Segundo os autores, o aumento da concorrência faz com que haja uma redução do poder der mercado que em associação com a responsabilidade limitada, tem como resultado, uma maior assunção de risco [27].

O estudo realizado por Boyd e Cihak [28] revela a intensidade da supervisão bancária poderia ser um impacto considerado na quantidade de risco assumido.

De uma forma geral, a empresa esforça-se para alcançar os resultados positivos. Que permitam atingir as metas detalhadas de determinadas partes interessadas. Assim, pode-se afirmar que um risco na empresa está relacionado com a probabilidade de ocorrência de eventos que resultem em perdas financeiras ou de outros recursos, percebidas como o desvio negativo dos resultados planeados.

Na perspetiva de longo prazo, o fluxo de lucro líquido é um ponto de partida para estimar o valor da empresa, independentemente do tipo de método utilizado para a estimativa.

Assim, o risco tem uma grande influência também no objetivo de longo prazo do empreendimento que é a maximização de valor [29].

A própria gestão de risco é um processo que geralmente é composto por quatro etapas: identificação (1), avaliação (2), atividades relativas ao risco (3) e controlo do risco (4). Dentro do estágio de identificação, as fontes de risco particulares são classificadas de acordo com vários critérios que deveriam, pelo menos, considerar o interior e o exterior do empreendimento [30].

A avaliação possibilita a seleção de fontes de risco em termos da probabilidade de ocorrência e do tamanho das consequências potenciais, de modo que as atividades relativas ao risco abranjam apenas as fontes mais graves para o resultado e o valor da empresa.

Na prática, e nos estágios referidos, as empresas estabelecem procedimentos individuais de gestão de riscos que, especialmente em grandes entidades, são matematizados e informatizados, o que facilita o processo de avaliação de riscos e a seleção de ações preventivas para limitar o risco.

Os sistemas mais complexos e modernos são os sistemas holísticos os Enterprise Risk Management (ERM), que funcionam com base na análise de big data, permitindo uma gestão de risco precisa e multifacetada [31].

Devido à variedade, ao ajuste individual e à natureza que consome o custo da implementação, os sistemas de ERM são considerados a melhor opção e a ferramenta

mais eficaz para a gestão de riscos que é tradicionalmente usada pela maioria das grandes empresas e corporações internacionais [31].

A identificação e a avaliação de riscos ocorrem com o uso de métodos quantitativos e / ou qualitativos. Métodos quantitativos gerais são métodos probabilísticos, estatísticos e econométricos. O primeiro método mencionado é baseado na teoria da probabilidade. Com O seu uso, pode-se avaliar a probabilidade de ocorrência de determinadas fontes de risco no futuro.

A empresa, tendo informações sobre ameaças e perdas (oportunidades e lucros) pode adicionalmente determinar a escala de resultados de ocorrência de risco. No entanto, o uso da teoria da probabilidade requer o conhecimento da frequência passada ou estimada de eventos e as informações sobre os resultados desses eventos. No primeiro caso, a informação utilizada traz, por vezes, uma suposição falsa sobre a repetibilidade do passado, enquanto no segundo caso a informação não pode prever com precisão o futuro [32].

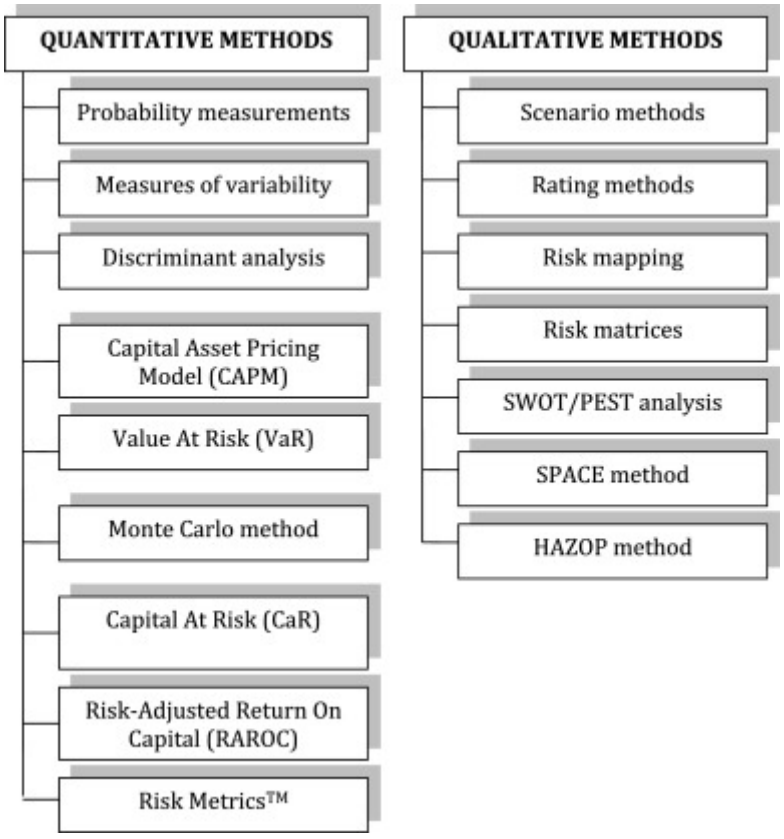


Figura 8 - Diferenças entre métodos qualitativos e quantitativos

Cennamo e Santaló [33] definem as plataformas multilaterais como “redes que reúnem dois ou mais tipos distintos de utilizadores e facilitam as transações entre eles”. Ou seja, as plataformas multilaterais são interfaces que podem servir para mediar transações entre dois ou mais lados. Estas definições demonstram que a noção de criação de valor através das plataformas de multicamadas depende da ativação de interações entre diferentes lados do mercado.

As plataformas multi-sided não se apropriam de produtos, mas dependem de recursos como as habilidades, ideias e ativos físicos, bem como as atividades controladas e fornecidas por agentes em diferentes lados do mercado. Ou seja, o papel de uma plataforma multilateral não é desenvolver, fabricar ou revender produtos e serviços, mas conectar diferentes lados de um mercado.

No caso de uma plataforma de dois lados, a lógica é que a maior base instalada de produtores oferece produtos na plataforma e conduz a uma maior necessidade por essa plataforma e, concomitantemente, ter mais consumidores leva a uma maior oferta de produtos [34].

Outro conjunto de pesquisas sobre as plataformas examinou a relação de valor interdependente em plataformas por um conjunto multilateral de parceiros, especialmente no contexto de plataformas como a Apple iOS ou o Mozilla Firefox, que fornecem um padrão com um núcleo tecnológico sobre o qual uma comunidade de utilizadores constrói [35].

Os estudos nesta corrente de literatura têm-se focado em mecanismos estruturais e evolutivos, bem como no alinhamento de parceiros que permitem a co-criação de valor, incluindo a gestão e coordenação de complementos para uma plataforma.

3

3. Tecnologia e Método de Desenvolvimento

3.1 OutSystems

Outsystems[2] é uma empresa portuguesa que fornece uma plataforma que permite às empresas desenvolver, alterar e manter aplicações empresariais. A plataforma de *low-code* desensolvida, que permite o desenvolvimento visual em toda a aplicação, facilmente integra com sistemas existentes, assim como adicionar código personalizado quando for preciso para o bom funcionamento da aplicação. Com esta plataforma é possível desenvolver aplicações tanto para telemóvel como para sites.

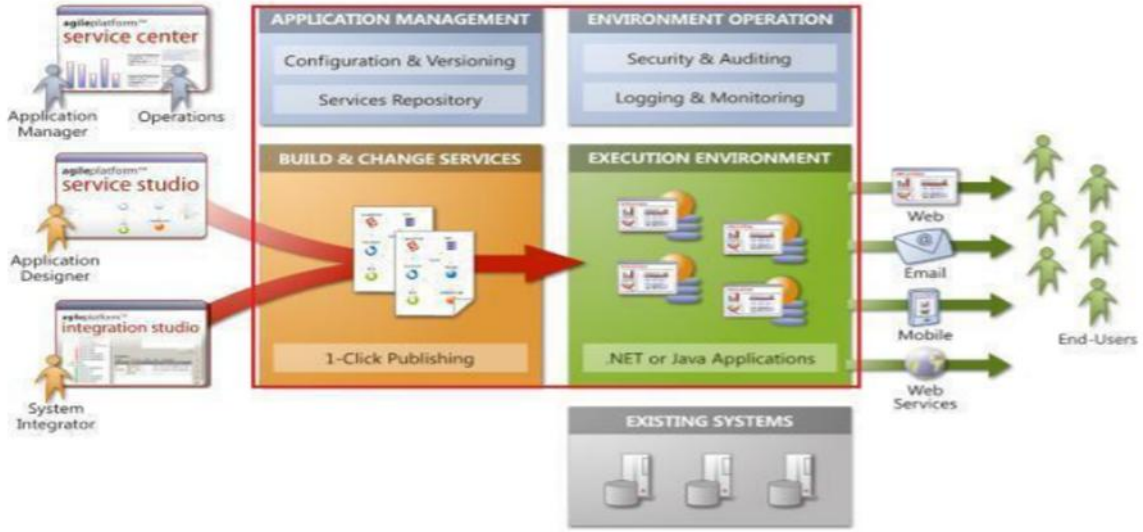


Figura 9 - Plataform OutSystems

A plataforma OutSystems foi fundada no ano de 2001, em Lisboa, Portugal, em San Ramon e Atlanta e Benelux, Maarssen Holanda. Tem a capacidade principal de permitir uma rápida inovação por meio de uma solução que integra e facilita a aplicação, o desenvolvimento, entrega, gestão e mudança.

A tecnologia OutSystems associa a produtividade oferecida pelas ferramentas de modelagem visual com o nível de extensibilidade que está presente na integração e estruturas de desenvolvimento personalizadas.

[2] http://www.outsystems.com/

OutSystems Agile Platform disponibiliza tudo o que a empresa precisa para criar e implementar de forma rápida os aplicativos de negócios e alterá-los em qualquer estágio do seu ciclo de vida.

Através do OutSystems Service é possível implementar aplicativos de negócios da Web, usando um ambiente de design intuitivo e visual. São acessíveis fluxos de integração do utilizador, modelos de dados, regras de negócios, processos agendados, serviços da Web e integração de adaptadores dentro de um ambiente visual.

A plataforma é constituída pelos seguintes módulos ilustrados na **Figura 9**:

• Service Studio – É um ambiente de desenvolvimento visual, para o desenvolvimento de aplicações que estão sujeitas a alterações nos seus processos de negócio. O service studio tem todos os componentes para a construção da aplicação, sem a necessidade de ter qualquer código escrito. Esta permite criar, alterar e publicar automaticamente as aplicações.

• Service Center – É uma consola web que permite ao programador de OutSystems gerir e monitorizar toda a plataforma ágil. Com isto é possível configurar políticas de controlos de acesso, realizar um controlo de qualidade sobre as equipas de desenvolvimento e sobre as aplicações, um histórico com todas as versões das aplicações realizadas e monitorizar e auditar a execução problemas de desempenho e qualidade.

• Integration Studio –Ambiente de trabalho para os programadores integrarem aplicações e acessos a bases de dados externas a partir de componentes identificar bases de dados, bibliotecas de APIs, componentes SAP e é possível usar o Micrsoft Visual Stutio para integração. Permite também criar conectores para integrar outros sistemas já existentes e que depois de integrados podem ser reutilizados em qualquer aplicação de OutSystems através do Service Studio.

• Plataform Server – Neste ambiente as aplicações são armazenadas, publicadas e executadas, e disponibiliza um conjunto de serviços para compilar e monitorizar as aplicações. Este ambiente está representado a vermelho na **Figura 9**.

A abordagem do OutSystems Agile é composta pelos seguintes estágios, conforme representado pelo gráfico abaixo:

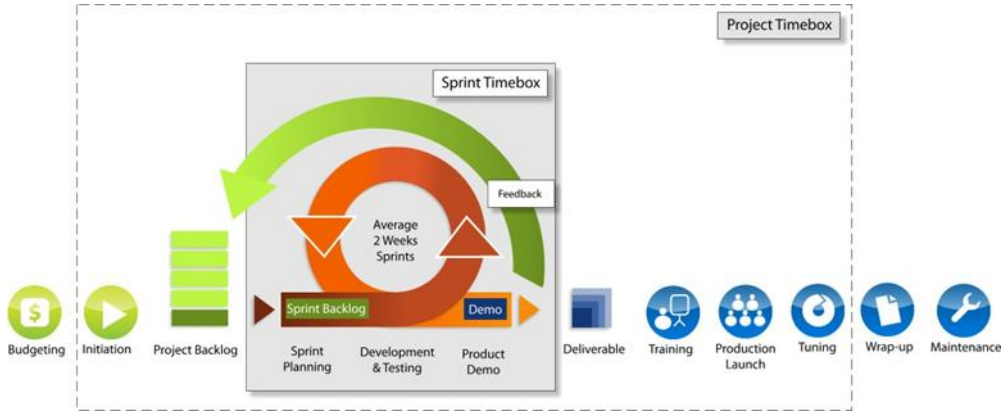


Figura 10 - Abordagem de OutSystems Àgil

1. Orçamento

2. Iniciação do Projeto

3. Desenvolvimento Iterativo - Planejamento, Desenvolvimento e Testes de Sprint e Demonstração do Produto

4. Treinamento

5. Lançamento da Produção

6. Ajuste

7. Encerramento

8. Manutenção

Esta tecnologia apresenta um conjunto de características essenciais para um desenvolvimento ágil. Tais como;

- Ter uma rapidez invencível, ou seja, desenvolve as aplicações ao nível visual e torna o processo mais rápido, e no final para implementar a solução na Cloud é necessário somente um clique com o rato.

- Grande escalabilidade, as várias aplicações que são desenvolvidas no OutSystems apresentam um ótimo desempenho, independentemente do número de utilizadores, da complexidade ou volume de dados
- A implementação não é quebrável, ou seja, a plataforma OutSystems somente deixa implementar as soluções que não têm erros, e assim, as aplicações nunca irão guardar soluções com erros nos ambientes da Cloud e no próprio ambiente.
- Segurança integrada, tem a capacidade de garantir que as aplicações estejam seguras desde o design até à implementação com os recursos de segurança mais recentes
- Integração com o todo, sendo fácil a ligação das aplicações desenvolvidas na plataforma com qualquer outro sistema

Importa ainda referir que o planeamento de sprint é a primeira atividade do estágio iterativo de desenvolvimento. Ou seja, a atividade de planeamento do sprint envolve e revê o blacklog do projeto e colabora com os membros da equipa de negócios para decidir quais os requisitos do utilizador. Este processo é designado de Liquidação do Backlog da Sprint. Durante este processo de negociação e priorização de recursos o gerente de negócios e o responsável pelo projeto estabelecem as prioridades para o sprint e equilibram o tempo total do projeto.

3.2 Método

Tendo em conta que a ferramenta teria que ser feita com a tecnologia OutSystems, de modo a ir ao encontro dos interesses da INCM, e que o método que esta tecnologia utiliza para desenvolvimento, é o scrum [41], impôs-se usar este método ágil para o desenvolvimento da aplicação.

Scrum é metodologia ágil e flexível para o desenvolvimento de um projeto. É uma metodologia de desenvolvimento de software que utiliza uma prática iterativa e incremental, como tal é possível ter uma melhor perceção de todo o desenvolvimento do projeto ao longo do tempo. Esta metodologia de desenvolvimento foca-se em entregar o mais rápido possível as funcionalidades com maior valor ao cliente, deste modo adapta-se a projetos onde os requisitos podem mudar rapidamente.

A **Figura 11** mostra o funcionamento da metodologia scrum. É composto pelos seguintes importantes conceitos:

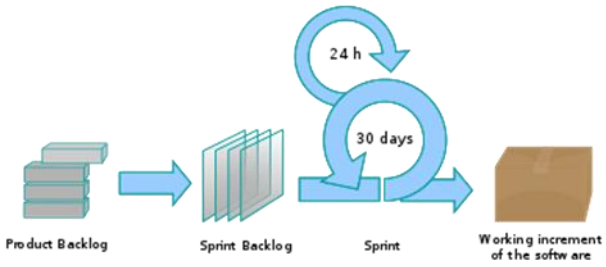


Figura 11 - Metodologia Scrum

- Product backlog: Lista que contém todas as funcionalidades de um produto.
- Sprint: Corresponde ao período, normalmente duas a três semanas no máximo quatro, onde são realizadas um conjunto de funcionalidades. No final de cada período, é feita uma entrega tangível e incremental.
- Sprint backlog: conjunto de funcionalidades e tarefas que a equipa compromete-se a fazer num Sprint, ordenadas por prioridade.

- Scrum meeting: Reunião que ocorre várias vezes durante o Sprint para monitorizar o progresso e os obstáculos.
- Scrum meeting rules: Conjunto de regras que formam um protocolo a seguir durante as reuniões de um Sprint.

Como a **Figura 11** demonstra, esta metodologia propõe que o projeto se inicie com uma lista de funcionalidades desejadas pelo cliente. Esta lista pode ser modificada pelo cliente a qualquer altura do projeto, e é dividida em tarefas que são desenvolvidas ao longo dos ciclos de 30 dias denominados por sprint.

Durante um sprint são realizadas reuniões entre os membros de equipa para discutir questões sobre o progresso e obstáculos do projeto. Idealmente estas reuniões seriam realizadas diariamente, mas devido à disponibilidade dos envolvidos, e após reflexão conjunta, definiu-se que seria mais proveitoso para todos se as reuniões fossem no máximo semanais, e visto que este projeto terá apenas um programador (autor do relatório) seria difícil ter todos os dias novas funcionalidades desenvolvidas para serem apresentadas e discutidas entre todos. O método continua a ser ágil tendo em conta que o contacto será constante durante o desenvolvimento, e desta forma possibilita maximizar os recursos existentes com o tempo disponível[3]. No final de cada ciclo encontram-se implementadas as funcionalidades previstas para o cliente poder testar. Desta forma é possível obter o parecer do cliente, que permite futuros ajustamentos do projeto. Este ciclo repete-se até à entrega final do produto.

Existem três papéis chaves na metodologia scrum:

- Product Owner: pessoa responsável pelo product backlog, que define quais as funcionalidades com maior prioridade e elege as tarefas a fazer aos restantes elementos da equipa. É a pessoa responsável por definir os sprints até ao desenvolvimento final do produto.
- Scrum Master: Gestor da equipa que garante que as tarefas são feitas pelos diferentes membros da equipa sem inconvenientes, e responsável pela equipa seguir boas práticas. Representa a equipa na presença do product owner.

[3] Artigo sobre alternativa a metodologia Scrum, Simon Kneafsey, em: http://www.scrum.org/resources/blog/itpossible-be-agile-without-using-scrum

- Team Member: Membro que faz parte da equipa de desenvolvimento do produto que tem como função tornar as tarefas do sprint backlog em funcionalidades.

A equipa de trabalho é constituída apenas por um elemento – autor do relatório. O trabalho foi mediado por outro elemento – co-orientador da INCM. O papel desempenhado por este elemento consiste em acompanhar o trabalho realizado pelo autor, através da elucidação de questões relacionadas com determinados componentes do projeto. O orientador deste projeto desempenha o papel de scrum master, com o objetivo de orientar a equipa de modo a chegar ao produto final.

4

4. Análise do problema

Nesta secção é explicada a estrutura da gestão de risco, que neste momento está definida na INCM [36].

4.1. Contexto do problema

Para promover a criação de valor da gestão de risco e com a finalidade de assegurar que todas as tomadas de decisão tenham em conta a informação de risco pertinente, bem como os princípios de gestão de risco devem estar em consonância com a missão e estratégica da INCM. Assim, existem um conjunto de princípios essenciais, como:

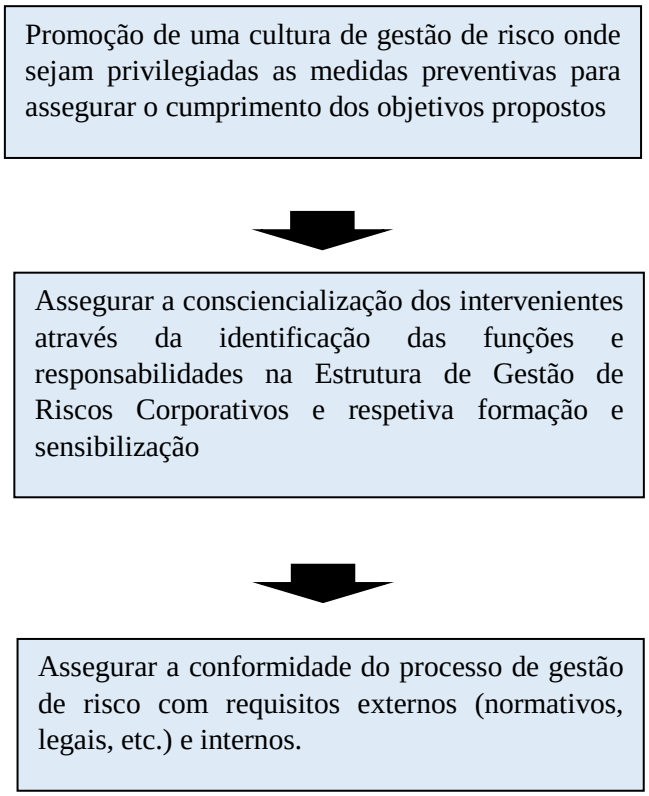


Figura 12 - Princípios gerais para a promoção da criação de valor da gestão de risco

Ao nível funcional, a gestão de riscos corporativos está representada na **Figura 13** e as funções de cada elemento são:

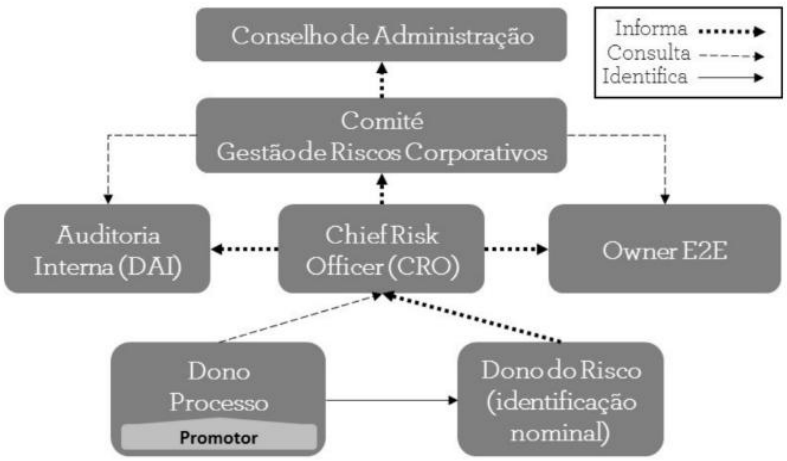


Figura 13 - Gestão de riscos Corporativos

• **Conselho de administração:** Apoiado pelo comité de gestão dos riscos corporativos, define a estratégia da gestão de risco. Fornece e aprova também recursos necessários para a gestão de riscos.

• **Comité de gestão de riscos corporativos:** Órgão que apoia o conselho de administração, acompanha e a estrutura de gestão de riscos, sugerindo alterações, seguindo uma estratégia de melhoria contínua. Garante a comunicação estre as partes interessadas.

• **Chief risk officer (CRO):** Define a estrutura da gestão risco, tendo que ser aprovada pelo comité de gestão corporativos. Dá suporte à implementação da estrutura de gestão de riscos da gestão de risco, como membro consultor, através da consolidação, agregação e categorização da informação de riscos.

• **Auditoria interna:** Órgão que avalia o processo da gestão de risco, "incluindo a correta identificação, análise, avaliação e tratamento dos riscos", [36]. Tendo em conta os riscos associadas este órgão tem como função priorizar os trabalhos do plano de auditoria.

• **Owners E2E:** Controla a informação de risco relativa à cadeia de valor e garante que as alterações feitas à cadeia são refletidas e comunicadas.

• **Dono do risco:** Monitoriza possíveis alterações aos riscos, quantifica os riscos residuais e assegura e avalia a eficácia dos controlos.

• **Dono do processo:** Órgão responsável pela identificação, análise e avaliação dos riscos.

4.2. Análise do Estado Atual

De uma forma geral, os objetivos principais para a gestão de riscos corporativos são estabelecidos de acordo com os objetivos estratégicos da INCM, por meio da definição das categorias de risco que se deseja abordar

Assim, ao nível estratégico, Governance e responsabilidade ambiental, o risco está relacionado com a alteração no ambiente, adversa ou benéfica, que resulta total ou parcialmente dos aspetos ambientais da organização.

No que respeita à responsabilidade social, o risco de uma decisão pode influenciar de forma positiva ou negativa, o desenvolvimento sustentável e o bem-estar da sociedade.

O risco de prática de um qualquer ato ou a sua omissão, seja neste caso lícito ou ilícito, contra o recebimento que não seja devido para o próprio ou para terceiros trata-se de uma corrupção ou infração conexa.

Com o objetivo de assegurar a uniformização da gestão de risco estabelece-se as seguintes atividades na gestão do risco corporativo:

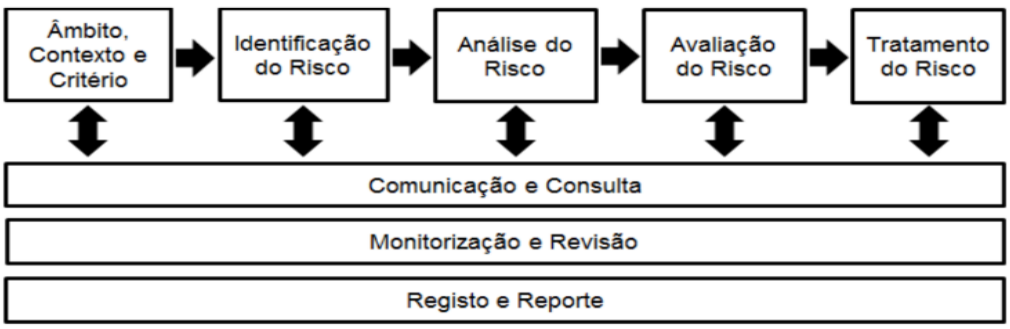


Figura 14 - Processo de Gestão de Risco Corporativo

5

5. Análise dos requisitos e desenho do caso de motivação

Nesta secção é apresentado o modelo de domínio e são também descritos os requisitos funcionais definidos pela INCM que foram implementados, conforme acordado com a entidade. De seguida são apresentados e detalhados os casos de uso que provêm dos requisitos funcionais escolhidos. Por último a descrição do desenvolvimento da ferramenta em tecnologia OutSystems é apresentada detalhadamente.

5.1 Análise do Modelo de Domínio

A análise e a recolha de informação da estrutura de ERM da INCM permitiu a construção de um modelo específico de domínio. O resultado está ilustrado na figura seguinte

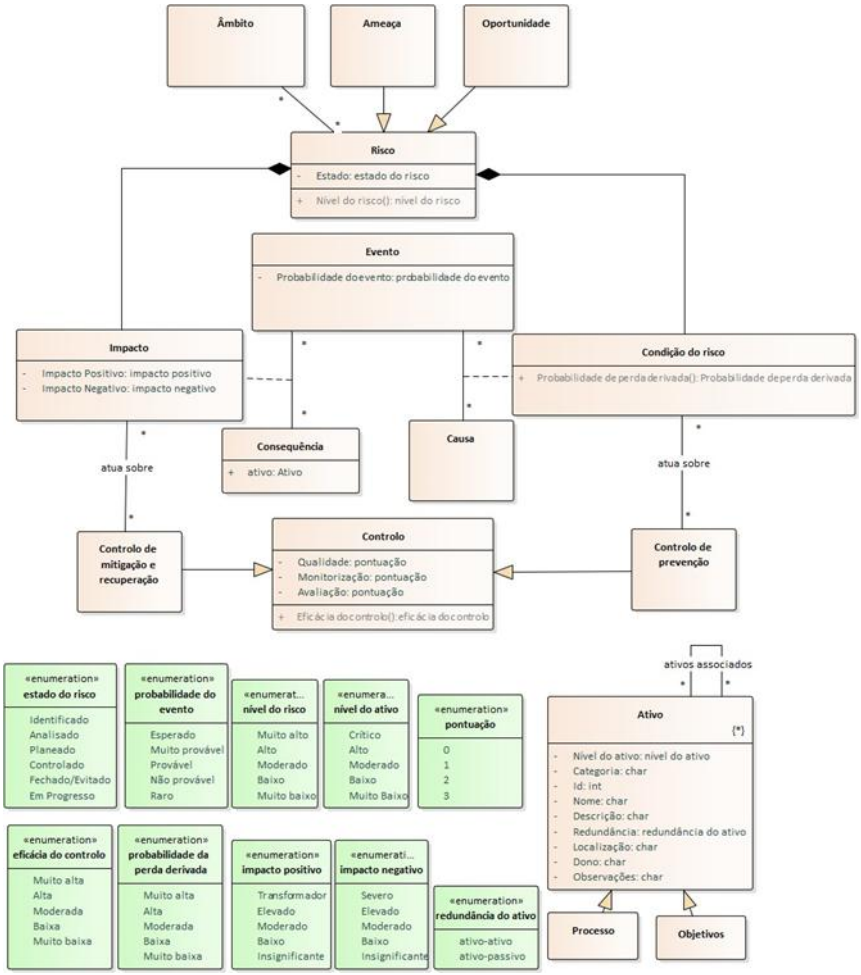


Figura 15 - Modelo de domínio da estrutura da ERM da INCM

As estruturas de ERM diferenciam-se de organização para organização adequando-se ao seu contexto e, desta forma algumas das associações, classes e respetivos atributos e escalas resultam do contexto em que a INCM se insere e estão definidas em [36].

Não obstante tem-se como principais conceitos as classes de âmbito e risco, em que o âmbito corresponde ao propósito da gestão de risco, e que pode ser mais do que um. No caso da INCM, o âmbito mais amplo é o do risco corporativo que inclui, igualmente, os âmbitos mais especializados como os âmbitos da segurança de informação (Certificação ISO27001 [37]), gestão da qualidade (certificação ISO9001), gestão ambiental (certificação ISO14001 [38]) e da produção gráfica de segurança (certificação ISO14298 [39]), etc.

De igual modo, o risco possui um atributo, o estado de risco que indica em que fase do seu ciclo de vida se encontra, e a operação nível de risco, tal como está apresentado na tabela seguinte.

Operação	Parâmetro(s) - Classe	Tipo de retorno
Nível do risco	• Impacto Máximo – Impacto • Probabilidade de perda derivada – Condição do risco	nível do risco
Probabilidade de perda derivada	• Probabilidade do evento – Evento • Eficácia do controlo – Controlo de prevenção	probabilidade de perda derivada
Eficácia do controlo	• Qualidade – Controlo • Monitorização – Controlo • Avaliação – Controlo	eficácia do controlo

Tabela 1 - Operações das classes do modelo de domínio

A classe de risco deriva de duas classes, a condição de risco que é constituída pela operação probabilidade de perda derivada, e o impacto que possui os atributos de impacto positivo e impacto negativo.

5.2 Requisitos Funcionais

Nesta secção são apresentados os requisitos que se desenvolveram durante a dissertação que estão definidos pela INCM [40], é possível ver todos os requisitos definidos em Apêndice A, mesmo os que se decidiu que não seriam implementados, pelo menos por agora.

Passando ao contexto da Gestão de Risco na INCM que é caracterizado na atualidade pela existência de várias Estruturas de Gestão de Risco Especializadas, cada uma focada em dar respostas concretas a necessidades operacionais (por exemplo, para obtenção de certificações) ou de negócio (por exemplo, para resposta a concursos nacionais e internacionais). Deste modo, a Estrutura de Gestão de Riscos Corporativos deverá visar ter como objetivo o desenvolvimento de uma ferramenta que, tirando vantagem das Estruturas de Gestão de Risco Especializadas já existentes, deverá permitir oferecer num dado momento uma visão comum e transversal dos riscos operacionais e de negócio da organização.

Para satisfazer esses objetivos é necessário resolver uma contradição: por um lado que a organização adote conceitos e princípios de gestão de risco comuns, enquanto por outro lado tal não pode constringir a definição de Processos de Gestão de Risco Especializados para os diversos contextos de negócio da organização. Esta contradição pode, no entanto, ser aparente se for conseguido desenhar e por em prática uma infraestrutura para uso comum, isto é, de uma solução tecnológica para gestão de um Registo de Riscos e com capacidade de geração de Relatórios de Risco, que sirva ao mesmo tempo cada contexto especializado e o objetivo da Gestão de Risco Corporativo. Isto é, uma infraestrutura que possa gerir toda a informação de risco de forma uniforme e transparente para as partes interessadas em cada um dos contextos, ao mesmo tempo que lhes garante serviços de suporte às suas atividades do Processo de Gestão de Risco, incluindo Relatórios de Risco, segundo as reais necessidades do respetivo contexto.

Para suportar a implementação do Processo de Gestão de Risco e o modelo de domínio comum à organização é necessário definir uma adequada infraestrutura de suporte. A Gestão de Risco Corporativo na INCM será suportada por um sistema de informação que irá ajudar na definição e integração de Registo de Riscos. Um Registo de Riscos é um objeto onde a informação de risco é registada. Mais concretamente, é uma ferramenta de suporte considerada essencial para a comunicação, consulta,

monitorização e revisão dos riscos – os principais objetivos da gestão de risco corporativo.

O Registo de Riscos é também a base para a integração da informação. Através dos diversos registos de Riscos criados pelos diferentes processos de Gestão de Risco, o sistema de informação a implementar deve permitir a agregação de toda a informação num Registo de Risco Corporativo. De maneira a possibilitar tal agregação é necessário que todos os registos de riscos criados tenham, pelo menos, os conceitos definidos para o registo corporativo. É importante referir que tipicamente a governação de risco apenas tem preocupações com riscos que ponham em causa o funcionamento da organização. É, portanto, necessário que a agregação permita também filtrar a informação de risco com base nas preocupações das partes interessadas, o que pode ser obtido através do estabelecimento do contexto por objetivos. Ou seja, deve ser concebido um Registo de Riscos de tal forma que possam ser listados e analisados Riscos relevantes para apenas um ou mais objetivos determinados.

Será necessário desenvolver um Back Office, com um "Serviço de utilizadores e grupos", de modo a garantir que a aplicação apenas é utilizado por pessoas previamente autorizadas para aceder ao sistema é necessário garantir uma boa gestão de utilizadores. Para simplificar a gestão de utilizadores, os requisitos abaixo introduzem o conceito de grupo de utilizadores que permite agrupar utilizadores por denominadores comuns.

Também irá ser desenvolvido um Front Office com um "Serviço de registo de risco", que corresponde a um processo de gestão de risco é suportado por um registo de risco - um objeto onde toda a informação de risco é registada. Mais concretamente, é uma ferramenta de suporte considerada essencial para a comunicação, consulta, monitorização e revisão dos riscos – os principais objetivos da gestão de risco corporativo. Front Office será também constituído por um serviço de relatórios de risco.

5.3 Casos de uso da aplicação

A presente secção descreve os principais casos de uso que afetam as classes presentes no modelo de domínio da aplicação. A **Figura 16** ilustra os casos de uso (UC[4]) identificados seguindo-se a descrição em formato textual e em tabela de cada um dos casos de uso identificados.

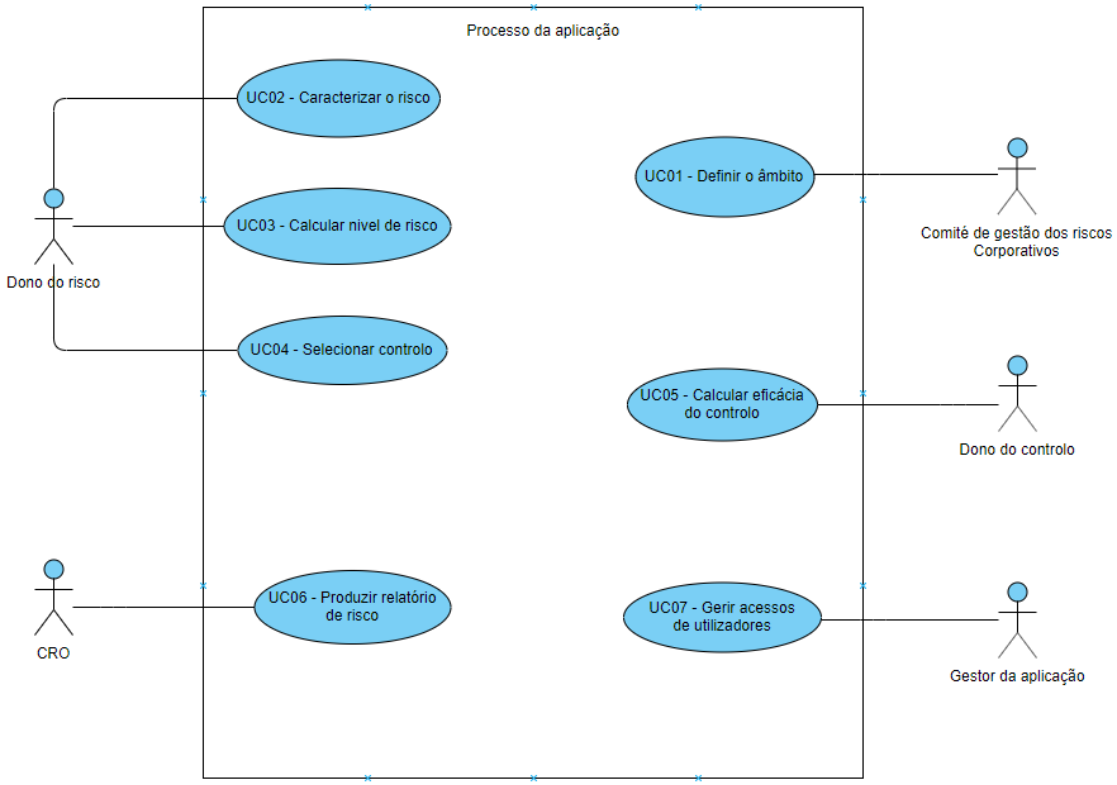


Figura 16 – Casos de uso do sistema

Pela análise da **Figura 16** identificam-se sete casos de usos distintos. Todos eles utilizam e/ou alteram classes presentes no modelo de domínio **Figura 15**.

Para cada um dos casos de uso ilustrados a cima serão de seguida detalhados em formato tabela de modo a descrever os seus atributos:

- **Caso de uso**. Apresenta o nome do caso de uso de acordo com a **Figura 16**;
- **Participante(s).** Define os atores que fazem parte do caso de uso;

[4] Tradução do acrónimo UC – Use Case

- **Pré-condições**. Define o conjunto de condições necessárias para que o caso de uso se possa concretizar;
- **Pós-condições**. Define o conjunto de condições que terão de ocorrer para que o caso de uso termine, nomeadamente que artefactos foram produzidos e/ou modificados e que classes do modelo de domínio fizeram parte do caso de uso;
- **Cenário principal**. Descrevem com maior detalhe o conjunto de ações que fazem parte do caso de uso.

Caso de uso: Definir o âmbito
Participante(s): CGRC
Pré-condições:
Pós-condições: Registo do risco atualizado com o âmbito das atividades da gestão do risco
Cenário Principal: 1. CGRC define o âmbito das atividades da gestão do risco 2. CGRC define os contextos interno e externo das atividades da organização 3. CGRC determina os critérios do risco que pretende seguir durante a sua operacionalização 4. CGRC regista o âmbito no Registo do risco

Tabela 2 - Descrição do caso de uso UC01

O caso de uso UC01, descrito na **Tabela 2**, descreve a fase do processo onde o CGRC define o âmbito das atividades de risco da organização, que inclui a definição dos contextos internos e externos. Assim que o âmbito se encontre definido este deve ser registado na aplicação de Registo de Risco.

Caso de uso: Caracterizar o risco
Participante(s): Dono do risco
Pré-condições: Novo(s) risco(s) comunicado(s)
Pós-condições: Registo do risco atualizado com os eventos, consequências, causas e controlos existentes (de prevenção e de mitigação e recuperação)
Cenário Principal: 1. Novo risco é comunicado 2. Dono do risco caracteriza o risco (os eventos, consequências, causas e controlos existentes) 3. Dono do risco regista características do risco no Registo do risco

Tabela 3 - Descrição do caso de uso UC02

O caso de uso UC02, descrito na **Tabela 3**, corresponde à fase do processo onde o Dono do Risco caracteriza o(s) novo(s) risco(s) que foram comunicados. Nesta caracterização dos novos riscos são associados os eventos, consequências, causas e controlos existentes.

Caso de uso: Calcular nível de risco
Participante(s): Dono do risco
Pré-condições: Conclusão do caso de uso UC02
Pós-condições: Probabilidade de perda derivada, impacto máximo e nível do risco registados no Registo do risco
Cenário Principal: 1. Inclui UC01 2. Dono do risco calcula probabilidade de perda derivada 3. Dono do risco calcula impacto máximo 4. Dono do risco calcula nível do risco 5. Dono do risco regista resultados no Registo do risco

Tabela 4 - Descrição do caso de uso UC03

O caso de uso UC03, descrito na **Tabela 4**, descreve a fase do processo onde o Dono do risco depois de ter caracterizado o(s) novo(s) risco(s) que foram comunicados, calcula o nível do risco. Para o cálculo do nível de risco o Registo de Risco calcula primeiro a probabilidade de perda derivada, utilizando para isso as métricas probabilidade do evento e a eficácia do controlo de prevenção, e de seguida o impacto máximo. O nível do risco é calculado através da interseção entre a probabilidade de perda derivada e o impacto máximo. Todos os resultados são registados no Registo do risco.

Caso de uso: Selecionar controlo
Participante(s): Dono do risco
Pré-condições: Conclusão do caso de uso UC05
Pós-condições: Registo do risco atualizado as categorias dos riscos, os controlos selecionados
Cenário Principal: 1. Dono do risco categoriza o(s) risco(s) em causa 2. Dono do risco seleciona os riscos considerados aceitáveis 3. Dono do risco seleciona os controlos existentes para os riscos não aceitáveis 4. Dono do risco regista no Registo do risco as novas informações geradas sobre os riscos

Tabela 5 - Descrição do caso de uso UC04

O caso de uso UC04, descrito na **Tabela 5**, descreve a fase do processo onde o Dono do riscos seleciona os controlos existentes para o(s) risco(s). Para tal é necessário que as eficácias dos controlos já tenham sido calculadas anteriormente.

Caso de uso: Calcular eficácia do controlo
Participante(s): Dono do controlo
Pré-condições:
Pós-condições: Atributo(s) do(s) controlo(s) e eficácia do(s) mesmo(s) registadas no Registo do risco
Cenário Principal: 1. Dono do tratamento planeia os tratamentos selecionados 2. Dono do tratamento implementa os tratamentos selecionados 3. Dono do tratamento verifica a qualidade dos tratamentos 4. Dono do tratamento regista qualidade dos tratamentos no Registo do risco

Tabela 6 - Descrição do caso de uso UC05

O caso de uso UC05, descrito na **Tabela 6**, descreve a fase do processo onde o Dono do Controlo calcula a eficácia do controlo aplicado. Nesta fase do processo o Dono do controlo irá planear e implementar os controlos selecionados. O planeamento dos controlos inclui as atividades de estimar o custo/benefício do controlo e data prevista da conclusão da implementação do controlo, entre outras. O caso de uso termina com a verificação da qualidade do controlo e com o registo destas métricas no Registo de Risco, que as irá usar para calcular a eficácia de um controlo.

Caso de uso: Produzir relatório do risco
Participante(s): CRO
Pré-condições: ocorrência do evento que despoleta o início da produção do relatório
Pós-condições: Comunicação da informação relativa a: riscos ; listagem com riscos agrupados ou ordenados pelo seu nível de risco, probabilidade ou impacto, riscos agrupados por causa, evento ou consequência; monitorização e implementação dos controlos de risco implementados
Cenário Principal: 1) CRO produz o relatório do risco 2) CRO partilha relatório produzido com as partes interessadas

Tabela 7 - Descrição do caso de uso UC06

O caso de uso UC06, descrito na **Tabela 7**, descreve a fase do processo onde o CRO elabora os relatórios de risco. Este caso de uso despoleta no início da produção do relatório que depois serão partilhados com as partes interessadas.

Caso de uso: Gerir acessos de utilizadores
Participante(s): Gestor da aplicação
Pré-condições:
Pós-condições: Gerir os acessos de todos os utilizadores que estejam criados na aplicação de forma a dar permissões adequadas a cada um deles.
Cenário Principal: 1) É pedida ao gestor da aplicação permissões para usar a aplicação 2) Gestor procura pelo utilizador em causa 3) Gestor dá as permissões necessárias em causa

Tabela 8 -Descrição do caso de uso UC07

O caso de uso UC07, descrito na **Tabela 8**, descreve a fase do processo onde o Gestor da aplicação fornece/retirar permissões aos utilizadores da aplicação ao definir os perfis que cada utilizador tem.

5.4 Desenvolvimento

Para este desenvolvimento foram realizados 3 ciclos cada um de 3 semanas, onde duas semanas correspondem a desenvolvimento, e a ultima semana corresponde a testes com o cliente.

No **primeiro ciclo** foi desenvolvido o serviço para gerir os acessos aos utilizadores (caso de uso UC07 – **Tabela 8**), criadas as entidades para o modelo de domínio, criadas páginas para definir o âmbito, criar relações entre entidades, e construção de matrizes de risco (caso de uso UC01 – **Tabela 2**).

Foram criados 5 perfis, porque existem 5 atores diferentes nos casos de uso definidos anteriormente, que são definidos como Roles em OutSystems:

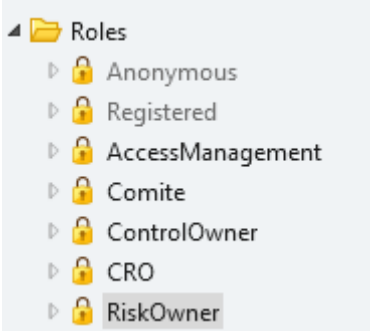


Figura 17 - Perfis em OutSystems

Depois de analisado o modelo de domínio desenvolvido com colega Tiago [42],este foi o modelo de dados feito em OutSystems, cada tabela de dados, em OutSystems, refere-se a Entidades, como está representado a seguir:

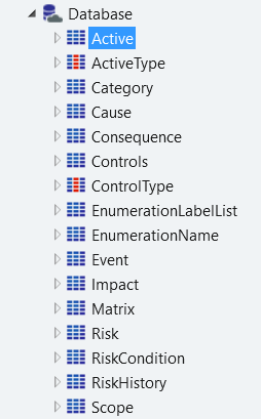


Figura 18 - Entidades do modelo de domínio

Na entidade **EnumerationName** são guardados todos o Enumerados, e na Entidade **EnumerationLabelList** são guardadas todas as labels de cada Enumerado, esta Entidade tem um atributo **EnumerationName** que referencia a qual o Enumerado, de modo a saber que label pertence a que Enumerado.

A Entidade Matriz é usada para guardar os dados para construir as matrizes entre Enumerados.

A entidade scope é usada para guarda o Scope de toda aplicação. Ou seja, associa os Enumerados criados na tabela **EnumerationName** a todos os Enumerados usados em toda aplicação.

Entidade **Controls** é composta por 3 atributos que depois é usado para calcular a eficácia do controlo. Esta entidade também tem um atributo que referencia a Entidade Estática **ControlType** para definir se o controlo é de **Prevenção** ou de **Mitigação e Recuperação**.

A entidade **Risk**, tem um Estado de risco, e tem mais dois atributos que referenciam para a Entidade **Impact** e a Entidade **RiskCondition**. Com estas relações é calculado o **Risk Level** que depois é também guardado como atributo na Entidade Risco.

Na Entidade **Impact** são guardados os Impactos positivos e negativos, e referencia o Evento associado assim como a consequência e o controlo.

RiskCondition referencia a causa, e evento e controlo associados. A probabilidade de perda derivada é calculada através da probabilidade do evento e a eficácia do controlo associado. A probabilidade de perde derivada é guardada nesta entidade.

Na entidade **Consequence** é referenciada a entidade **Active**. Nesta entidade **Active** são guardadas algumas informações básicas, como a categoria, a descrição, a localização, dono do risco, etc.

Foi criado um ecrã de gestão de utilizadores, disponível no separador **Access Management**, que serve para gerir as roles associadas a cada utilizador da aplicação (Para aceder a esta página precisa de ter o role **Access Management**):

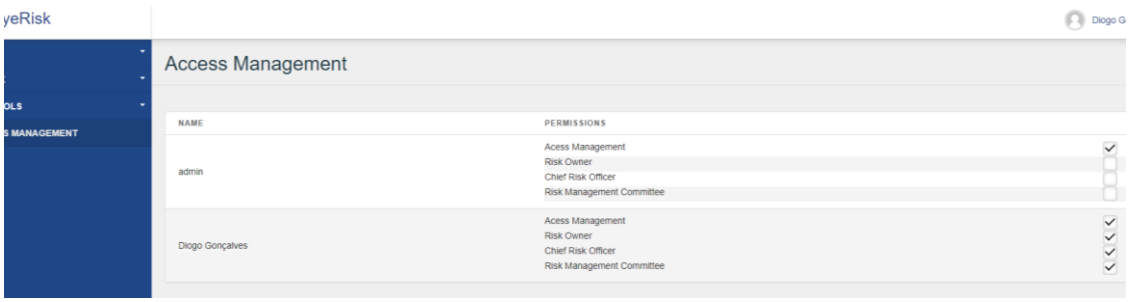


Figura 19 - Gestão de acessos da aplicação

É possível definir o Âmbito no ecrã para definir o Scope, para que fosse garantido que apenas a pessoa responsável por definir âmbito tivesse permissões para editar. (Para aceder a esta pagina precisa de ter o role **Risk Management Committee**):

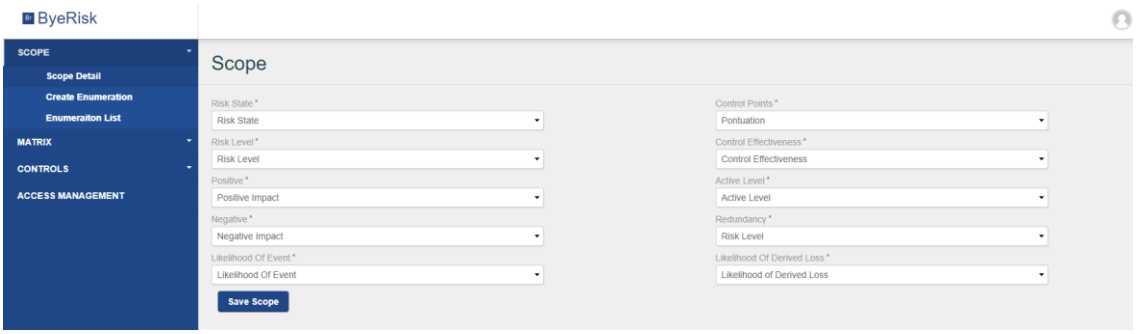


Figure 20 - Definição do âmbito da aplicação

Cada label como a que se segue é feita através de uma combo box, onde a source de cada combo box é uma lista de todos os Enumerados criados na aplicação (**Figura 38** em apêndice B).

Para criar um Enumerado apenas é preciso colocar um Nome, que já não exista, e é criado um Enumerado (**Figura 39** em apêndice B), na lista dos Enumerados (**Figure 21**) é possível editar através do ícone azul, apagar com a cruz vermelha ou então adicionar labels ao Enumerado através do "mais" verde, que nos leva para a página de adicionar labels (**Figura 40** em apêndice B) onde é possível adicionar labels desde que tenham sempre nomes e valores diferentes. É ainda possível editar (ícone azul) e apagar (ícone vermelho) labels criadas (Para aceder a estas páginas precisa de ter o role **Risk Management Committee**):

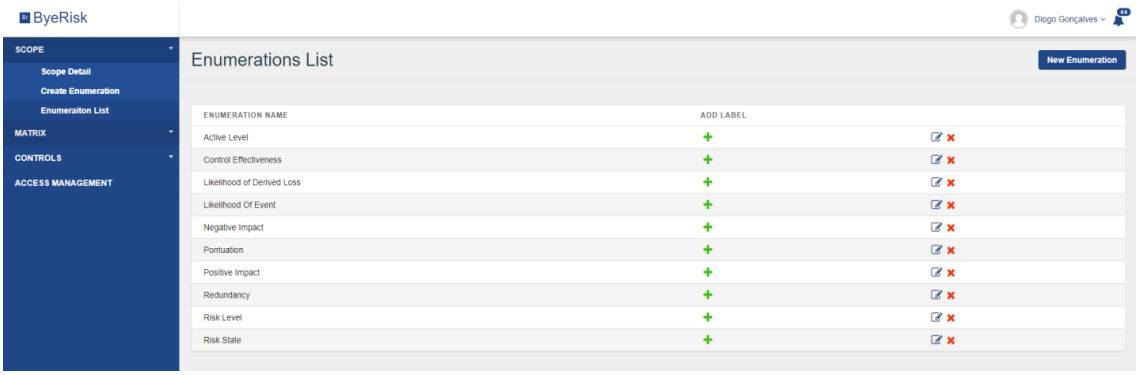


Figure 21 - Listagem dos Enumerados da aplicação

No Menu Matriz é possível criar relações (**Figure 41** em apêndice B), escolhendo os Enumerados que se pretendem relacionar e qual será o Enumerado do resultado e de seguida carregar no Continuar. Ao carregar no botão aparece então uma lista com as labels do primeiro Enumerado, e ao carregar no link **Relation** aparecerá uma popup com uma lista das labes do segundo Enumerado seguido com uma combo box, para colocar o resultado que irá resultar entra as labels em causa de cada Enumerado (**Figure 42** em apêndice B). Neste menu depois de ser criada as relações é possível gerar a matriz das relações criadas (**Figure 22**), para isto é preciso escolher os enumerados dos quais se pretende gerar a matriz e carregar no botão calcular criadas (Para aceder a estas paginas precisa de ter o role **Risk Management Committee**).

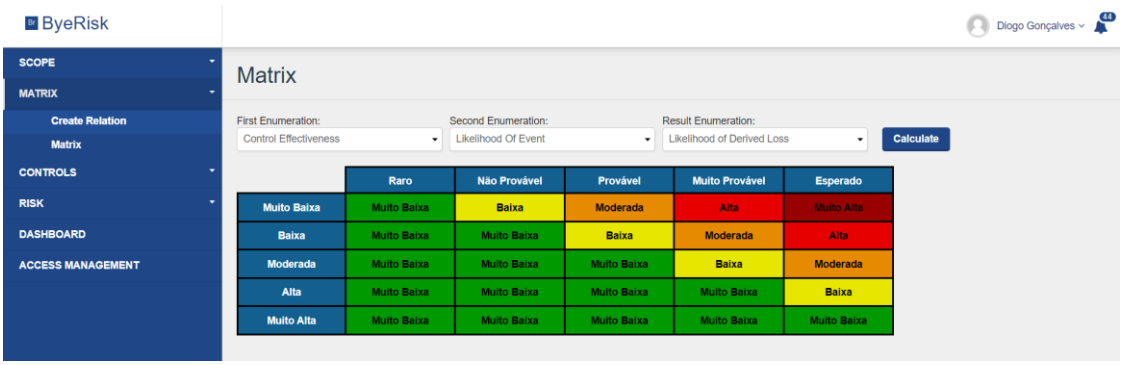


Figure 22 - Geração de matrizes da aplicação

No **segundo ciclo** de desenvolvimento foram criados ecrãs para criar e editar controlos (caso de uso UC05 – **Tabela 6**), ecrã com uma lista dos vários detalhes de um risco onde é possível editar cada um desse detalhes (caso de uso UC02 – **Tabela 3**), incluído consequências, causas, eventos e ativos.

No menu **Controls** é possível ver a lista de todos os controlos existentes. Nesta lista aparece o nome dos controlos, o tipo de controlo (**prevenção** ou **mitigação e recuperação**), qual a pontuação dada a cada um dos atributos (**qualidade**, **monitorização** e **avaliação**), a eficácia calculada através desses atributos. Ainda é possível editar (ícone azul - **Figure 23**), que é redirecionado para uma página de edição do controlo (**Figure 43** em apêndice B) e apagar um controlo (ícone vermelho - **Figure 23** figura X). Para criar um controlo carrega-se no menu **Create Control** ou então no botão **New Control** existente na lista de controlos no canto superior direito. No ecrã para criar um controlo (**Figure 44** em apêndice B), todos os campos são obrigatórios, sendo de preenchimento obrigatório o nome do controlo, o tipo e as suas **pontuações**, no final ao gerar o controlo será calculado a eficácia do controlo, como definida em [36], que aparece do lado direito. (Para aceder a estas paginas precisa de ter o role **Control Owner**).

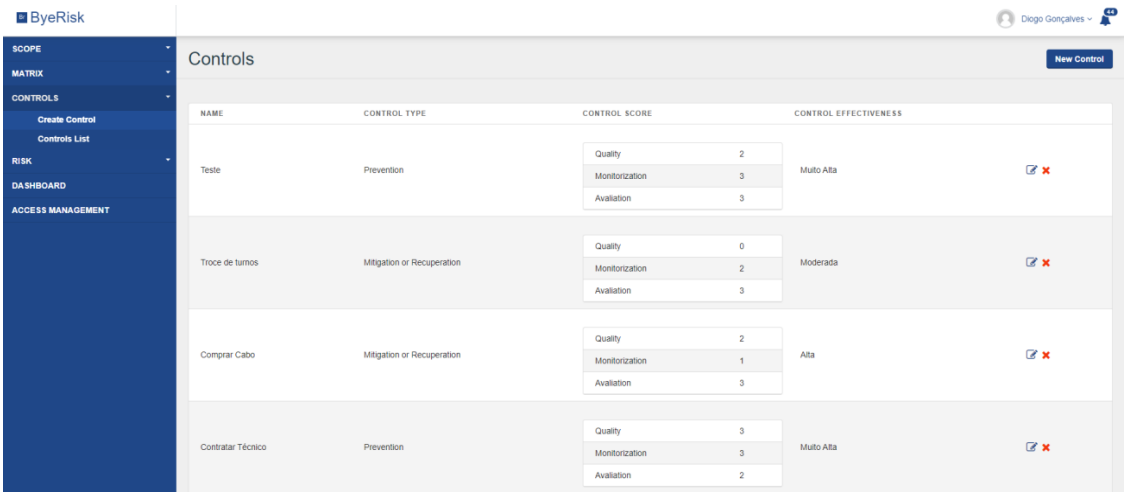


Figure 23 - Listagem de Controlos da aplicação

No ecrã de Lista de Detalhes de um risco (**Figure 24**), existem 4 listas, uma para cada detalhe (Evento, Cause, Consequência, Ativos). Em cada um destas listas existe um link para criar um novo detalho (**Figure 45** em apêndice B) na parte superior direita de cada lista, e ainda é possível editar (**Figure 45** em apêndice B) e apagar um detalhe com os ícones que se encontram na lista em cada uma das linhas. (Para aceder a estas paginas precisa de ter o role **Risk Owner**).

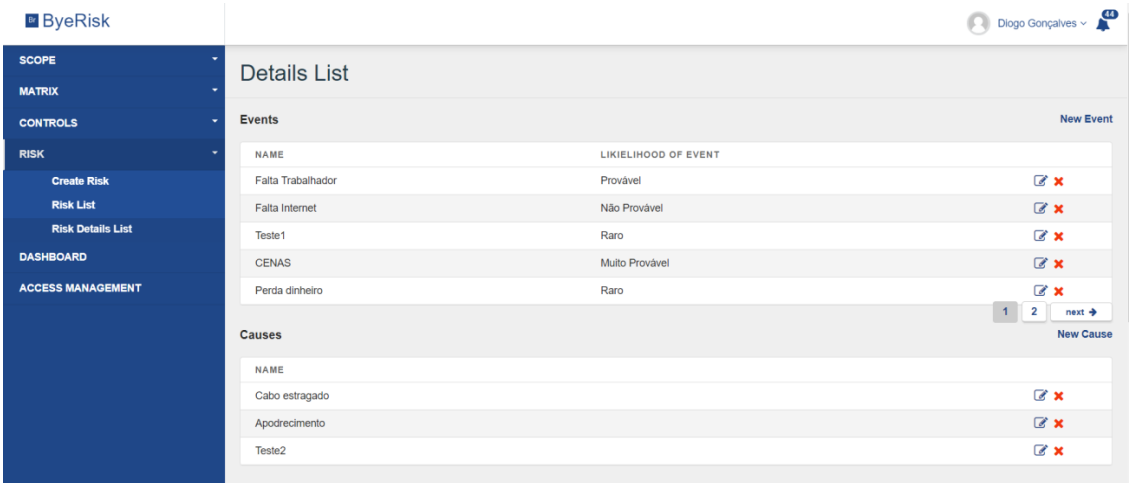


Figure 24 - Listagem de detalhe de um risco da aplicação

Para a **terceira e última fase de desenvolvimento**, foi criado um ecrã para o risco de risco (caso de uso UC03 – **Tabela 4**), onde é calculado o nível do risco a partir das matrizes definidas no âmbito, um Dashboard com informação geral sobre a gestão de risco, e um relatório que é possível exportar na página Dashboard (caso de uso UC06 – **Tabela 7**).

Para criar um Risco (**Figure 25**) é possível faze-lo acedendo pelo menu na separador **Create Risk**, neste ecrã é necessário preencher todos os campos de modo a gerar um risco, incluindo a seleção dos controlos adequados (caso de uso UC04 – **Tabela 5**), à exceção dos impactos que apenas é possível escolher ou um impacto negativo ou um impacto positivo (Para aceder a estas paginas precisa de ter o role **Risk Owner**):

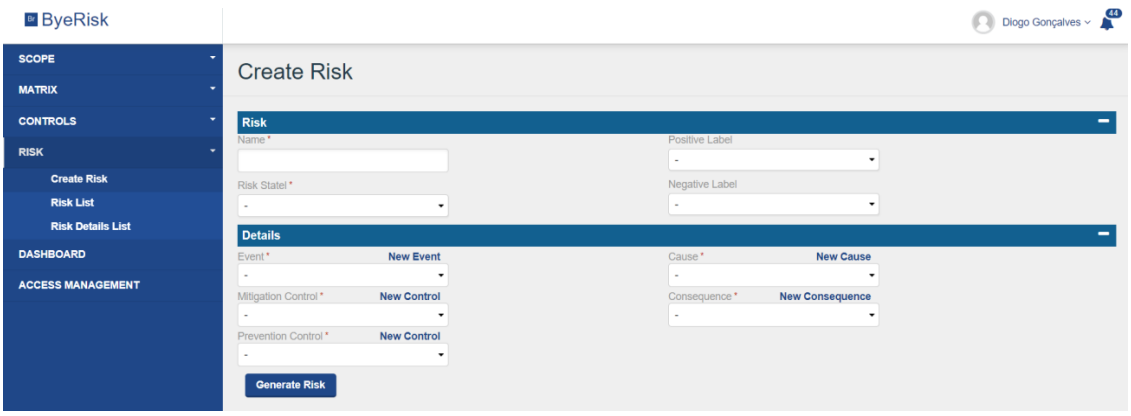


Figure 25 - Criação/Edição de um risco da aplicação

Na Listagem dos riscos (**Figure 26**) é possível ver todo os riscos existentes assim como algumas informações básicos sobre o próprio, sendo ainda possível editar e eliminar o risco pela tabela clicando nos ícones correspondentes (ícone azul para editar, ícone vermelho para apagar) (Para aceder a estas paginas precisa de ter o role **Risk Owner**):

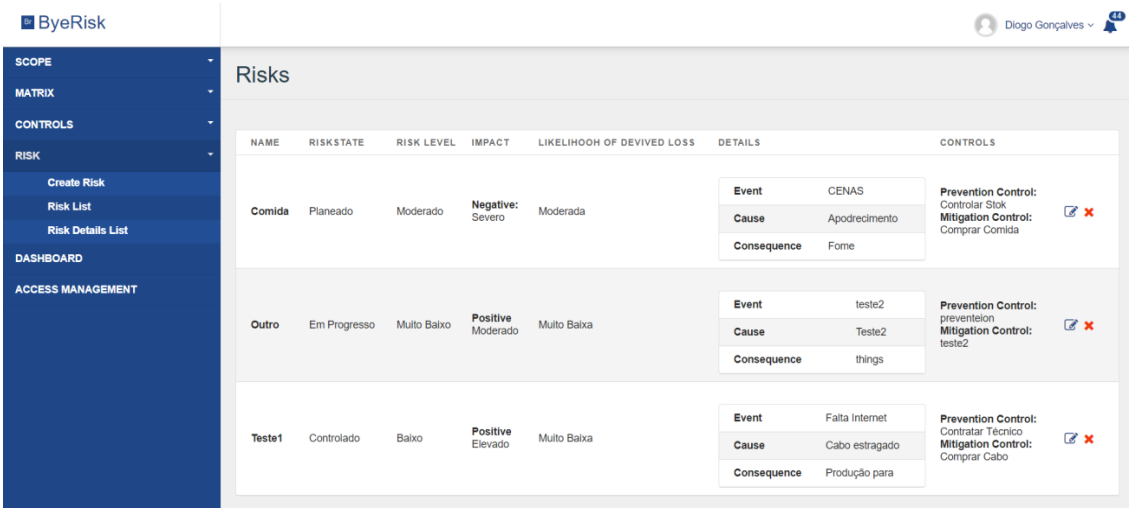


Figure 26 - Listagem de riscos da aplicação

No ecrã Dashboard (**Figure 27**) é possível ver os riscos identificados até aos momentos, assim como todos os riscos que foram mitigados e o nível global de risco [42], calculado em tempo real. Neste Dashboard existem outros níveis estatísticos, assim

como a eficácia dos controlos e o número de riscos que existem por nível (Para aceder a estas paginas precisa de ter o role **CRO**):

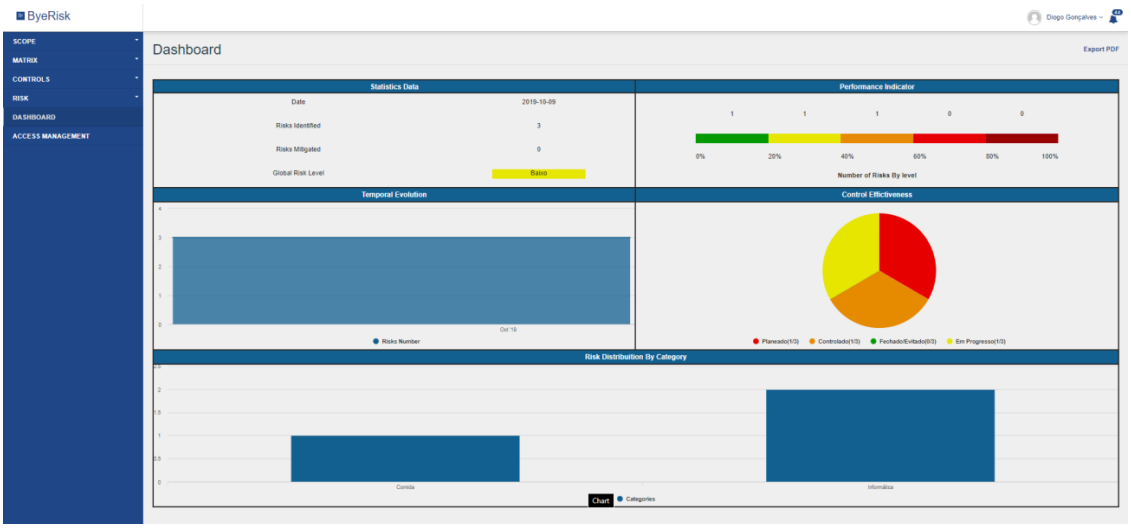


Figure 27 - Dashboard da aplicação

Clicando no botão **Export PDF** é gerado um relatório de risco em formato “pdf”, onde contêm as matizes de risco, as informações sobre todos os riscos existes, como algumas dados gerais que existem no Dashborad e ainda as matrizes que são utilizados para calcular o nível de risco e a probabilidade de perda derivada. (Para aceder a estas paginas precisa de ter o role **CRO**).

Para o desenvolvimento da exportação de um relatório pela aplicação, foi usado um componente existente na *forge* de OutSytems (HtmlToPDFConverter), que transforma uma página em Html, neste caso um webscreen criado em OutSystems, para pdf.

6

6. Demonstração da Solução

Como referido ao longo do documento devido a motivos de confidencialidade não foi possível ter acesso a dados da INCM para demonstrar a solução, apesar de o caso motivação corresponder ao caso real da INCM.

Em alternativa foi fornecido um caso artificial, de modo a poder demonstrar a solução com o mesmo sucesso que os dados da INCM teriam. Será portanto descrito o caso artificial numa primeira fase e de seguida demonstrado como os dados deste caso prático são utilizados na ferramenta desenvolvida.

6.1 Descrição do caso artificial

O caso retrata um cenário de uma pizzaria que serve comida tanto na sala de jantar como em entregas ao domicílio. O chefe de sala assistido por um empregado garante o serviço de sala. O empregado garante também a entrega ao domicílio com uma mota da pizzaria.

Os pedidos de entrega ao domicílio são recebidos por site, e o diretor recebe uma sms do próprio site. A pizzaria tem uma cozinha, orientada por uma chefe de cozinha, responsável por todas as encomendas que ele recebe do diretor. O chefe de cozinha tem um auxiliar que executa tarefas sobre a chefia do chefe de cozinha. Quando um pedido é concluído o chefe informa o diretor, se for um pedido ao domicílio o empregado prossegue para a entrega.

O assistente do chefe de cozinha é responsável pela contagem dos recursos existentes na cozinha, e o chefe é responsável por encomendar mais recursos quando assim for preciso. O assistente tem ainda como função, limpar a cozinha, e o empregado limpar a sala de jantar e verificar o estado da mota.

6.2 Demonstração da solução

Os dados que foram usados para demonstrar encontram-se em Apêndice C, como estes dados apenas se referem a todo o modelo de domínio da ferramenta menos a definição do âmbito, os dados para o âmbito foram usados conforme estão definidos no modelo de domínio, e a construção de matrizes foi feita conforme o documento [36] o descreve.

Para o UC01 da **Tabela 2** a definição de matrizes, é necessário cria-se relações no ecrã de criar relações, e escolher entre quais enumerados se vai criar relação e o enumerado que resulta da combinação destes dois. Por exemplo, multiplicando numa matriz a probabilidade de perde derivada com o impacto negativo obtêm-se o nível de risco para definir quais as entradas de cada um cria-se relações no em cada uma das entradas, com as figuras seguintes ilustram.

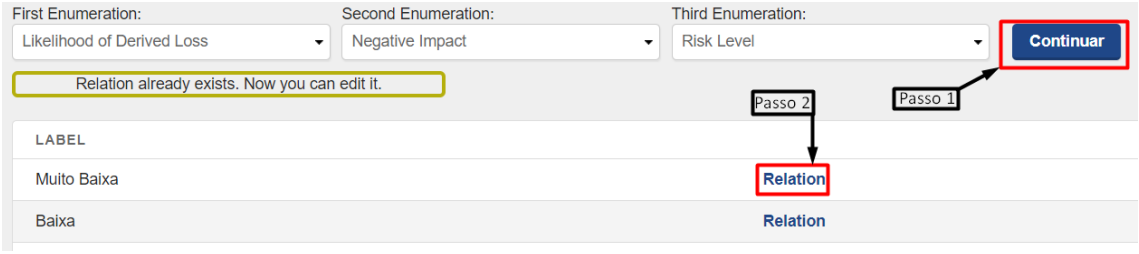


Figura 28 - Escolha de Enumerados

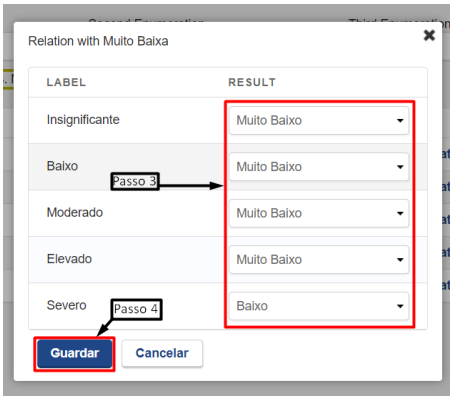
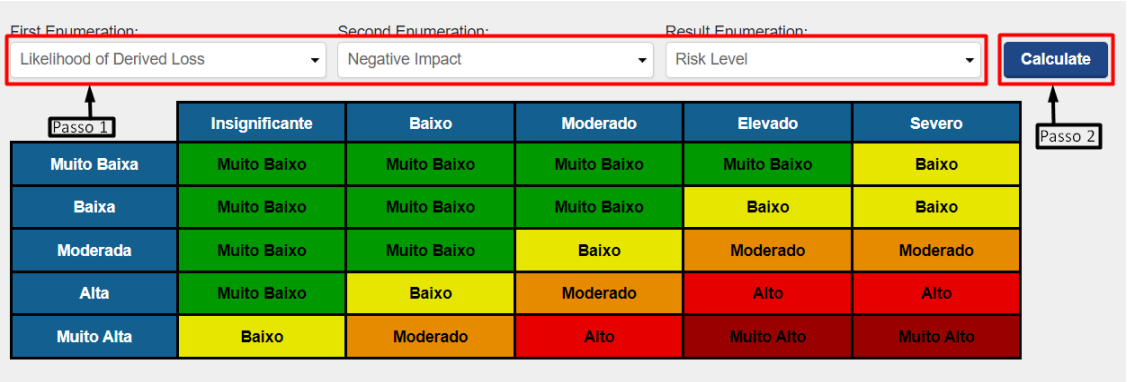


Figura 29 - Definição da matriz

De modo a ver o resultado obtido das relações criadas, no ecrã Matriz, escolhe-se os Enumerados em questão e com o botão calcular é gerada a matriz com é possível ver na seguinte figura:



	Insignificante	Baixo	Moderado	Elevado	Severo
Muito Baixa	Muito Baixo	Muito Baixo	Muito Baixo	Muito Baixo	Baixo
Baixa	Muito Baixo	Muito Baixo	Muito Baixo	Baixo	Baixo
Moderada	Muito Baixo	Muito Baixo	Baixo	Moderado	Moderado
Alta	Muito Baixo	Baixo	Moderado	Alto	Alto
Muito Alta	Baixo	Moderado	Alto	Muito Alto	Muito Alto

Figura 30 - Geração de Matriz

Passando ao UC05 da **Tabela 6**, é necessário aceder ao ecrã de criar controlos, colocar o nome do controlo, pontoar o controlo e definir se é controlo de prevenção ou de mitigação. Após isto gera-se o controlo e a ferramente calcular a eficácia desse mesmo controlo, como é demonstrado pela figura seguinte:

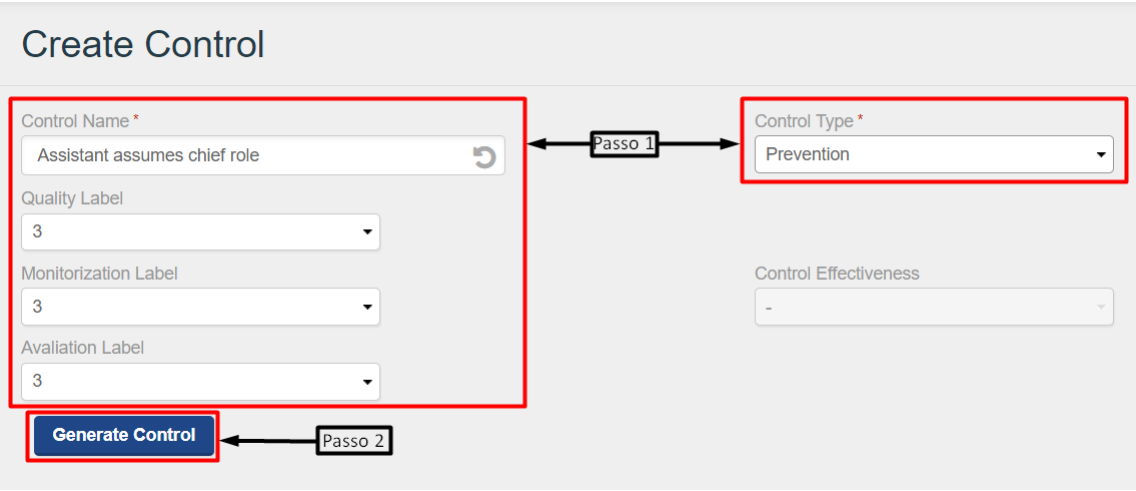


Figura 31 - Criação de Controlo

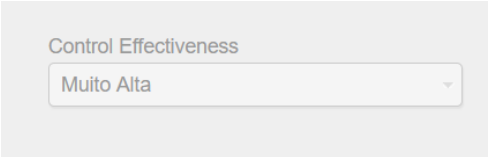


Figura 32 - Eficácia do controlo

No UC02 da **Tabela 3**, depois de abrir o ecrã para criar riscos é necessário identificar o risco, colocar o impacto positivo ou negativo, qual o estado do risco, como é demonstrado:

Figura 33 - Identificação de um Risco

É necessário também escolher/criar um evento, uma causa e uma consequência, como a seguinte figura demonstra um exemplo de criação de uma consequência:

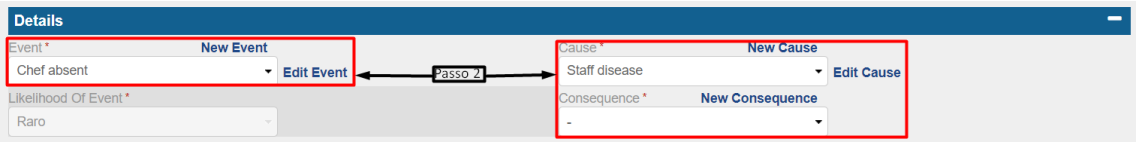


Figura 34 - Caracterização de um risco

De modo a concluir o UC04 da **Tabela 5**, é necessário ainda no ecrã de criação de risco selecionar qual o controlo de prevenção e qual o controlo de mitigação:

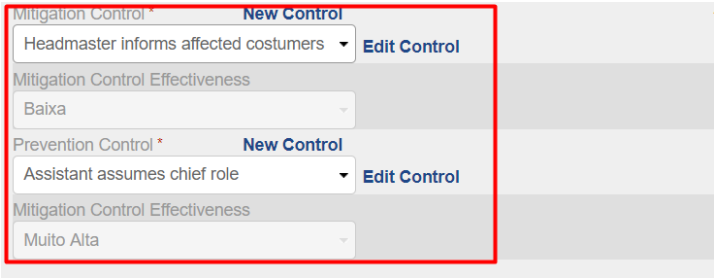


Figura 35 - Seleção dos controlos

Concluindo os casos de uso o ator "Dono do Risco" com o UC03 da **Tabela 4**, é necessário carregar no botão de gerar o risco, que é automaticamente calculado através das matrizes definidas no âmbito e a caracterização feito no risco, como se pode ver na figura seguinte:

Figura 36 - Calcular Nível de Risco

Por fim depois de todos os dados terem sido submetidos, ao navegar pela ferramenta até à página do Dashboard, clicando na ligação exportar para Pdf é gravado um relatório de risco que é automaticamente gravado no disco e que contêm as matrizes de risco, as matrizes utilizadas para o cálculo do nível de risco, o nível do risco global, indicador de performance e a listagem de todos os riscos.

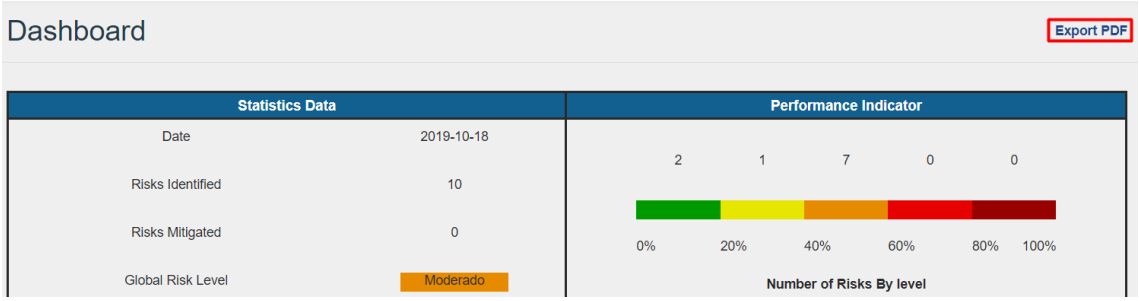


Figura 37 - Exportar PDF

Segue-se o relatório gerado:

Bye Risk

Risk Report

2019-10-23

Matrix

(Negative Impact x Likelihoof Of Event)

	Raro	Não Provável	Provável	Muito Provável	Esperado
Severo	4-7-9-10-11	8-12			
Elevado			13		
Moderado		5		6	
Baixo					
Insignificante					

(Likelihood Of Derived Loss x Negative Impact)

	Insignificante	Baixo	Moderado	Elevado	Severo
Muito Baixa			5-6	13	4-7-8-9-10-11-12
Baixa					
Moderada					
Alta					
Muito Alta					

(Control Prevention Effectiveness x Likelihood Of Event)

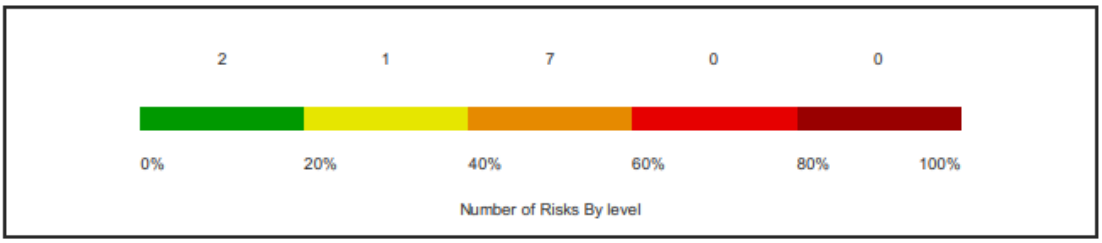
	Raro	Não Provável	Provável	Muito Provável	Esperado
Muito Baixa					
Baixa					
Moderada	9-10		13		
Alta					
Muito Alta	4-7-11	5-8-12		6	

Details

General Stats

Risks Identified	10
Risks Mitigated	0
Global Risk Level	Moderado

Performance indicator



Risks

NAME	RISKSTATE	RISK LEVEL	IMPACT	LIKELIHOOH OF DEVIVED LOSS	DETAILS		CONTROLS
Assistant absent - Risk Number: 5	Identificado	Muito Baixo	**Negative:** Moderado	Muito Baixa	**Event**	Assistant absent	**Prevention Control:** Trainee assumes assistant role **Mitigation Control:** Headmaster informs affected costumers
					Cause	Staff disease	
					Consequence	Food cannot be served in a causeable time	
Chef absent - Risk Number: 4	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**	Chef absent	**Prevention Control:** Assistant assumes chief role **Mitigation Control:** Headmaster informs affected costumers
					Cause	Staff disease	
					Consequence	Food cannot be produced	
Dinning room is not operational - Risk Number: 10	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**	Dinning room is not operational	**Prevention Control:** Backup power generator **Mitigation Control:** Headmaster informs affected costumers
					Cause	Power outage	
					Consequence	Food cannot be served in house	

Headmaster absent - Risk Number: 7	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**: Headmaster absent **Cause**: Staff disease **Consequence**: Food cannot be served in house	**Prevention Control:** Waiter assumes headmaster role **Mitigation Control:** Headmaster informs affected costumers
Home orders are not received - Risk Number: 12	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**: Home orders are not received **Cause**: Mobile phone network failure **Consequence**: Costumers fill complaint of home delivery service	**Prevention Control:** Home delivery by taxi **Mitigation Control:** Disccount vouchers given to affected costumers
Key ingredient not available - Risk Number: 13	Identificado	Baixo	**Negative:** Elevado	Muito Baixa	**Event**: Key ingredient not available **Cause**: Faillure in stock management **Consequence**: Food quality cannot be guaranteed	**Prevention Control:** Key ingredient replaced by alternative **Mitigation Control:** Identify supplyer for emergencies
Kitchen is not operational - Risk Number: 9	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**: Kitchen is not operational **Cause**: Power outage **Consequence**: Food cannot be produced	**Prevention Control:** Backup power generator **Mitigation Control:** Disccount vouchers given to affected costumers
Motorcyle is not operational - Risk Number: 11	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**: Motorcyle is not operational **Cause**: Motorcycle is broken **Consequence**: Home delivery cannot be fulfilled	**Prevention Control:** Home delivery by taxi **Mitigation Control:** Disccount vouchers given to affected costumers

Trainee absent - Risk Number: 6	Identificado	Muito Baixo	**Negative:** Moderado	Muito Baixa	**Event**	Trainee absent	**Prevention Control:** Assistant makes extra time **Mitigation Control:** Headmaster informs affected costumers
					Cause	Staff disease	
					Consequence	Food cannot be served in a causeable time	
Waiter absent - Risk Number: 8	Identificado	Moderado	**Negative:** Severo	Muito Baixa	**Event**	Waiter absent	**Prevention Control:** Trainnee assumes waiter role **Mitigation Control:** Headmaster informs affected costumers
					Cause	Staff disease	
					Consequence	Home delivery cannot be fulfilled	

Context

Matrix - Likelihood Of Derived Loss
(Control Prevention Effectiveness x Likelihood Of Event)

	Raro	Não Provável	Provável	Muito Provável	Esperado
Muito Baixa	Muito Baixa	Baixa	Moderada	Alta	Muito Alta
Baixa	Muito Baixa	Muito Baixa	Baixa	Moderada	Alta
Moderada	Muito Baixa	Muito Baixa	Muito Baixa	Baixa	Moderada
Alta	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa	Baixa
Muito Alta	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa

Matrix - Risk Level
(Likelihood Of Derived Loss x Postive Impact)

	Insignificante	Baixo	Moderado	Elevado	Transformador
Muito Baixa	Muito Baixo	Muito Baixo	Muito Baixo	Baixo	Moderado
Baixa	Muito Baixo	Muito Baixo	Baixo	Moderado	Moderado
Moderada	Muito Baixo	Baixo	Moderado	Moderado	Alto
Alta	Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Muito Alta	Baixo	Baixo	Alto	Muito Alto	Muito Alto

(Likelihood Of Derived Loss x Negative Impact)

	Insignificante	Baixo	Moderado	Elevado	Severo
Muito Baixa	Muito Baixo	Muito Baixo	Muito Baixo	Baixo	Moderado
Baixa	Muito Baixo	Muito Baixo	Baixo	Moderado	Moderado
Moderada	Muito Baixo	Baixo	Moderado	Moderado	Alto
Alta	Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Muito Alta	Baixo	Baixo	Alto	Muito Alto	Muito Alto

7

7. Conclusão

Este capítulo apresenta as conclusões finais da dissertação, bem como possíveis futuros passos para dar continuidade à mesma.

7.1. Conclusão

A gestão de risco implica um processo coordenando de medição de risco e gestão de risco. Este processo tem dois aspetos distintos, a avaliação de risco que a empresa enfrenta, como o risco de mercado, créditos, liquidez, e risco operacional. E integrada nos riscos de avaliação em várias localizações geográficas da empresa, ao nível legal. Ao nível de teoria, as duas dimensões devem ser dirigidas a produzir uma avaliação consolida de risco.

Na prática, existem poucas empresas que têm atualmente em vigor um sistema de gestão de risco consolidado que integra ambas as dimensões. Embora muitas instituições parecem dedicar os recursos significativos para o desenvolvimento destes sistemas. Assim sendo, a gestão de riscos refere-se ao total processo que uma instituição segue para definir um negócio.

O objetivo principal da gestão de riscos corporativos é criar um quadro de referência que permite às empresas lidar com o risco e incerteza. Os riscos são presentes em todas as atividades económicas e financeiras das empresas. O processo de identificação, avaliação e gestão são parte do desenvolvimento estratégico das empresas, pois deve ser concebida e planeada ao mais alto nível. Assim, uma abordagem integrada de gestão de riscos deve avaliar, controlar e monitorizar todos os riscos e as suas dependências para que a empresa avalie, controle e monitorize todos os riscos e incertezas.

Neste trabalho, foi feita uma análise ao processo descrito na norma ISO31000 e à estrutura de gestão de risco definida na INCM, e com isto foi construído um modelo de domínio em UML [43].

Com este modelo de domínio foi desenvolvida, em conjunto com a INCM, uma aplicação de uso para gestão de risco, fácil e intuitiva, que auxilia com o processo que a INCM tem definido.

7.2. Trabalho Futuro

INCM, como qualquer organização, vai sofrendo pequenas ou grandes alterações nos seus processos com a evolução dos tempos, como tal é necessário voltar a reunir com INCM regularmente de modo a manter a aplicação atualizada ao processo de gestão de risco e desta forma estabelecer novos desenvolvimentos.

Ainda dentro deste desenvolvimento que foi feito para a elaboração desta dissertação seria uma boa prática, rever com a INCM se o relatório que é exportado para PDF vai de encontro com as suas expectativas, assim como se não precisam de mais nenhum outro tipo de relatório. Na parte do "Dashboard" criar filtros para obter diferentes tipos de pesquisas.

Por último seria importante rever com a INCM todos os requisitos que estão definidos no documento que não foram desenvolvidos, de modo a perceber se neste momento fará sentido o desenvolvimento de mais algum dos requisitos.

Bibliografia

[1] Kedar, B. Z. (1970). Again: Arabic Risq, Medieval Latin Riscum. Studi Medievali. Centro Italiano di Studi Sull Alto Medioevo, Spoleto.

[2] Rowe, William (1977). An Anatomy of Risk, New York: John Wiley

[3] Merna, A e Merna, T (2004), 'Development of a model for risk management at corporate, strategic business and project levels', Journal of Structured and Project Finance, The, vol. 10, pp. 79-85.

[4] Flanagan, R. and Norman, G. (1993). Risk Management and Construction, Blackwell, Oxford.

[5] Buganova, K., Hudakova, M. (2015) Increase of the competitiveness of enterprises through the implementation of risk management projects in Slovakia

[6] Dingsoyr T., Nerur S., Balijepally V., Moe NB. (2012). A decade of agile methodologies: Towards explaining agile software development. J Syst Soft, 85: 1213-1221.

[7] Serrador, P.; Pinto, J. K. (2015) Does agile work? A quantitative analysis of agile project success. International Journal of Project Management, v.33, n.5, p 1040-1051.

[8] Kalus, G.; Kuhrmann, M. (2013) Criteria for software process tailoring: a systematic review. In: ACM. Proceedings of the 2013 International Conference on Software and System Process. [S.l.]. P. 171-180

[9] Campanelli AS. e Parreiras FS. (2015). Agile methods tailoring – A systematic literature review. J Syst Softw.110. p. 85-100

[10] Aven, T. (2012). Questões fundamentais na avaliação e gestão de riscos Risco Anal, 32 (10), pp. 1647 – 1656

[11] Pagach, D. e Warr, R. (2011). The characteristics of firms that hire chief risk officers, The Journal of Risk and Insurance, Vol 78, No.1, pp. 185-211

[12] Crader B. (2015). What makes an IT Project Successful? Nonprofit Edition. NpENGAGE.

[13] DeLone e McLean, E. R. (2016) Information Systems Success Measurement. Foundations and TrendsR in Information Systems, vol.2, no.1, pp. 1-116.

[14] Taylor, H. Artman E. e Woelfer JP. (2012) Information technology project risk management: bridging the gap between research and practice, Journal of Information Technology; 27:17–34

[15] Mahaney, R e Lederer, A. (2011). Effect of Intrinsic and Extrinsic Rewards for Developers on Information Systems Project. Eastern Kentucky University.

[16] Baccarini D. (1999) The logical Framework Method for Defining Project Success. Project Management Journal; 30(4): 25-32.

[17] Pimchangthong, D. e Boonjing, V. (2017). Effects of Risk Management Practice on the Success of IT Project. Procedia Engineering 182, 579-586.

[18] Instituto Português da Qualidade, (2018). NP ISO 31000. Gestão do risco. Linhas de orientação. Instituto Português da Qualidade.

[19] Alameida, A. B. de. (2011). Gestão da Água - Incertezas e Riscos. Conceptualização Operacional.

[20] Purdy, G. ISO 31000 (2009)—Setting a New Standard for Risk Management. Risk Analysis, v.30, n.6, p.881-886, 2010.

[21] Schwab, K. (2012) The Global Competitiveness Report, Full Data Edition is published by the World Economic Forum within the framework of the Global Benchmarking Network.

[22] Allen, F. e Gale, D. (1997). Financial Markets, Intermediaries, and Intertemporal Smoothing, Journal of Political Economy 105, 523-546.

[23] Rajan, R.G. (2005), Has Financial Development Made the World Riskier?, National Bureau of Economic Research Working Paper Series, No. 11728.

[24] Boot, A., Thakor, A.V., (2018). Commercial Banking and shadow banking: the accelerating integration of banks and markets and its implications for regulation. In: Berger, Allen, Mullineaux, Phil, Wilson, John (Eds.), chapter in Oxford Handbook of Banking, third ed. forthcoming

[25] Stiroh, K.J. (2010), "Diversification in Banking", in A. Berger, P. Molyneux and J. Wilson (eds.), The Oxford Handbook of Banking pp.146-171.

[26] Jimenez, G., Lopez, J. e Saurina, J. (2007). Como a concorrência afeta a assunção de riscos bancários?

[27] Hellmann, Murdock, K. e Stiglitz, J. (2000). Liberalization, Moral Hazard in Banking, and Prudential Regulation: Are Capital Requirements Enough? The American Review, Vol.90, No.1, pp. 147-167

[28] Boyd, J. H., De Nicolò, G. e Jalal, A. M. (2006). Bank risk-taking and competition revisited: New Theory and new evidence. International Monetary Fund, WP/06/297.

[29] Callahan, C. e Soileau, J. (2017). O gerenciamento de riscos corporativos melhora o desempenho operacional? Adv. Conta. 37, pp.122-139

[30] Stankiewicz-Mróz, A. (2015). Abordagem das questões de liderança nos processos de aquisições de empresas, 6ª conferência internacional sobre fatores humanos aplicados e ergonomia (AHFE 2015) e as conferências afiliadas, ahfe 2015 Procedia Manufac, pp. 793-798.

[31] Arena, M., Arnaboldi, T. e Palermo, T. (2017). A dinâmica do gerenciamento de risco (des) integrado: um estudo de campo comparativo Conta. Org. Soc. 62, p. 65-81.

[32] Hahn, J., DiLellio, A. e Dyer, JS. (2018). Prémio de risco em previsões de preço de commodities e seu impacto na avaliação Econ Econ. 72, pp. 393-403.

[33] Cennamo e Santaló, J. (2015). Como evitar armadilhas de plataforma MIT Sloan Manag. Rev, 57 (1) (2015), p. 12-15.

[34] Boudreau, K., e Jeppesen, L., (1777) Complementadores de multidões não remunerados: a miragem de efeito de rede de plataforma Estratégia. Manag. J. 36, pp.

[35] Adner, R. (2017). Ecossistema como estrutura: um constructo acionável para a estratégia J. Manag, 43 (1), p. 39-58.

[36] Vieira, R. (2018), PA18 - Descrição do processo. Framework de gestão de riscos corporativos, Relatório Interno, INCM.

[37] International Organization for Standardization, (2013) ISO/IEC 27001:2013, Information tecnology - Security techniques - Information security management systems - Requirements.

[38] Instituto Português da Qualidade (2016), NP EN ISO14001:2015, Sistemas de gestão ambiental. Requisitos e linhas de orientação para a sua utilização.

[39] International Organization for Standardization, (2013) ISO 14298:2013, Graphic technology -- Management of security printing processes.

[40] Vieira, R. (2018), Requisitos para o Sistema de Gestão de Risco Corporativo da INCM, INCM, Relatório Interno.

[41] Cardozo, E., Neto, J., Barza, A., França, A. e Silva, F. (2010) SCRUM and Productivity in Software Projects: A Systematic Literature Review.

[42] Santos, G. (2018). Enterprise risk management. Dissertação (Dissertação em Engenharia Informática e de Computadores), Instituto Superior Técnico.

[43] Ferreira, T. (2019). Modelação em CMMN do processo da gestão de risco. Dissertação (Dissertação em Engenharia Informática e de Computadores), Instituto Superior Técnico.

[44] Peffers, K. (2007), A Design Science Research Methodology for Information Systems Rsearch, Journal of Management Information Systems.

Apêndice A

Requisitos para o Sistema de Gestão de Risco Corporativo da INCM

1 Introdução

O contexto da Gestão de Risco na INCM é caracterizado na atualidade pela existência de várias **Estruturas de Gestão de Risco Especializadas**, cada uma focada em dar respostas concretas a necessidades operacionais (por exemplo, para obtenção de certificações) ou de negócio (por exemplo, para resposta a concursos nacionais e internacionais).

Deste modo, a **Estrutura de Gestão de Riscos Corporativos** deverá visar ter como objetivo o desenvolvimento de uma ferramenta que, tirando vantagem das Estruturas de Gestão de Risco Especializadas já existentes, deverá permitir oferecer num dado momento uma visão comum e transversal dos riscos operacionais e de negócio da organização.

Para satisfazer esses objetivos é necessário resolver uma contradição: por um lado que a organização adote conceitos e princípios de gestão de risco comuns, enquanto por outro lado tal não pode constringir a definição de **Processos de Gestão de Risco Especializados** para os diversos contextos de negócio da organização.

Esta contradição pode, no entanto, ser aparente se for conseguido desenhar e por em prática uma infraestrutura para uso comum, isto é, de uma solução tecnológica para gestão de um **Registo de Riscos** e com capacidade de geração de Relatórios de Risco, que sirva ao mesmo tempo cada contexto especializado e o objetivo da Gestão de Risco Corporativo. Isto é, uma infraestrutura que possa gerir toda a informação de risco de forma uniforme e transparente para as partes interessadas em cada um dos contextos, ao mesmo tempo que lhes garante serviços de suporte às suas atividades do Processo de Gestão de Risco, incluindo **Relatórios de Risco**, segundo as reais necessidades do respetivo contexto.

Para suportar a implementação do **Processo de Gestão de Risco** e o modelo de domínio comum à organização é necessário definir uma adequada infraestrutura de suporte. A Gestão de Risco Corporativo na INCM será suportada por um sistema de informação que irá suportar a definição e integração de Registo de Riscos. Um Registo de Riscos é um objeto onde a informação de risco é registada. Mais concretamente, é uma ferramenta de suporte considerada essencial para a comunicação, consulta, monitorização e revisão dos riscos – os principais objetivos da gestão de risco corporativo.

O Registo de Riscos é também a base para a integração da informação. Através dos diversos registos de Riscos criados pelos diferentes processos de Gestão de Risco, o sistema de informação a implementar deve permitir a agregação de toda a informação num **Registo de Risco Corporativo**. De maneira a possibilitar tal agregação é necessário que todos os registos de riscos criados tenham, pelo menos, os conceitos definidos para o registo corporativo. É importante referir que tipicamente a governação de risco apenas tem preocupações com riscos que ponham em causa o funcionamento da organização. É, portanto, necessário que a agregação permita também filtrar a informação de risco com base nas preocupações das partes interessadas, o que pode ser obtido através do estabelecimento do contexto por objetivos. Ou seja, deve ser concebido um Registo de Riscos de tal forma que possam ser listados e analisados Riscos relevantes para apenas um ou mais objetivos determinados.

Para garantir que as partes interessadas entendem e conseguem utilizar a informação de Risco, é essencial que todas as atividades de Risco envolvam a comunicação e consulta constante com essas partes. Neste contexto, a comunicação deve ser assegurada através da produção de **Relatórios de Risco**. Os Relatórios de Risco devem incluir toda a informação possível e necessária, estruturada e apresentada de acordo com as preocupações e necessidades do destinatário. Na Estrutura de Gestão de Risco Corporativo anteveem-se três tipos de Relatórios de Risco:

- **Relatórios de Risco Corporativo**, que devem informar o Comité de Risco dos Riscos corporativos identificados realçando riscos com um nível de risco elevado e que consequentemente requerem intervenção imediata;
- **Relatórios de Risco Especializado**, que devem informar as pessoas interessadas nos processos de gestão de risco especializado. Os relatórios de risco especializado tipicamente consistem em listas de riscos agrupadas ou ordenadas pelos elementos de risco identificados. Os Relatórios de Risco Especializado possíveis dependem do contexto do mesmo e especificamente do Registo de Risco (Domínio de Riscos) utilizado;
- **Relatórios de Mitigação de Risco**, devem informar os Donos do Risco dos riscos que afetam os seus ativos e dos controlos que se pretendem implementar para mitiga-los. Visto que diferentes processos de Gestão de Risco Especializado podem identificar riscos sobre os mesmos ativos, os Relatórios de Mitigação de Risco devem integrar a todos os riscos relacionados com o ativo independentemente do Processo de Gestão de Risco que os identificou.

2 Requisitos Funcionais

R2.1. O Sistema de Gestão de Risco Corporativo (SGRC) deve implementar as seguintes funcionalidades:

- Serviço de utilizadores e grupos;
- Serviço de papéis de utilizadores;
- Serviço de alertas de utilizadores;
- Serviço de modelo de domínio;
- Serviço de atributos de risco e escalas de valores;
- Serviço de registo de risco;
- Serviço de planeamento e tempo;
- Serviço de relatórios de risco;
- Serviço de risco corporativo;

Cada serviço pode ser implementado separadamente ou em conjunto.

2.1 Serviço de utilizadores e grupos

Para garantir que o SGRC apenas é utilizado por pessoas previamente autorizadas para aceder ao sistema é necessário garantir uma boa gestão de utilizadores. Para simplificar a gestão de utilizadores, os requisitos abaixo introduzem o conceito de grupo de utilizadores que permite agrupar utilizadores por denominadores comuns.

R2.1.1 O SGRC apenas pode acedido por utilizadores autenticados e ativos. A autenticação de um utilizador deve ser realizada com base num nome de utilizador e uma palavra passe.

R2.1.2. Um utilizador deve poder ser identificado, pelo menos, pela seguinte informação:

- Nome de utilizador;
- Palavra Passe;
- Tipo de utilizador;
- Estado (ativo ou inativo);
- Localização;
- Departamento;
- Endereço de correio eletrónico;
- Companhia;
- Contacto;
- Descrição do utilizador.

R2.1.3. O SGRC deve suportar um processo para criar utilizadores com a informação indicada no requisito R2.1.2.

R2.1.4. O SGRC deve suportar um processo para alterar a informação identificada no requisito R2.1.2 exceto nome de utilizador;

R2.1.5. O SGRC deve suportar um processo para recuperar a palavra passe de um utilizador.

R2.1.6. O SGRC deve suportar um processo para adicionar ou remover utilizadores a um grupo de utilizadores.

R2.1.7. O SGRC deve suportar um processo para desativar utilizadores. Um utilizador desativado é mantido no sistema mas com o estado inativo.

R2.1.8. O SGRC deve suportar um processo para eliminar utilizadores. Um utilizador eliminado é removido do sistema.

R2.1.9. O SGRC deve permitir a criação de grupos com, pelo menos, a seguinte informação:

- Nome do grupo;
- Estado (ativo ou inativo);
- Descrição do grupo;
- Utilizadores que pertencem ao grupo.

R2.1.10. O SGRC deve suportar um processo para alterar a informação identificada em R2.1.9.

R2.1.11. O SGRC deve suportar um processo para destruir um grupo de utilizadores. Um grupo destruído é mantido no sistema mas com o estado inativo.

R2.1.12. O SGRC deve suportar um processo para eliminar um grupo de utilizadores. Um grupo eliminado é removido do sistema.

R2.1.13. A destruição ou eliminação de um grupo de utilizadores pode, ou não, destruir ou eliminar os utilizadores que a ele pertencem dependendo da escolha do utilizador.

2.2 Serviço de papéis de utilizadores

Uma Estrutura de Gestão de Risco tipicamente envolve múltiplas partes interessadas com diferentes preocupações sobre o Processo de Gestão de Risco. Adicionalmente, a gestão de risco pode envolver informação com diferentes níveis de permissão. Para gerir as diferentes preocupações e permissões é necessário que o SGRC possua um sistema de permissões baseado em papéis de utilizadores. Um papel de utilizador é um conceito que permite definir um conjunto de permissões tipicamente associado a uma função no processo de gestão de risco.

R2.2.1. O SGRC deve permitir que um utilizador autorizado possa criar papéis de utilizadores com a seguinte informação:

- Título;
- Descrição;
- Administrador (Sim ou Não);
- Permissões.

R2.2.2. O SGRC deve permitir que um utilizador autorizado possa alterar a informação identificada no requisito R2.2.1.

R2.2.3. O SGRC deve permitir que um utilizador autorizado possa eliminar um papel de utilizador desde que este não esteja associado a um utilizador.

R2.2.4. O SGRC deve permitir que um utilizador autorizado possa definir, pelo menos, as seguintes permissões:

- Autorização para criação, alteração e eliminação de domínios;
- Autorização para criação, alteração e eliminação de atributos de risco em domínio especificado;
- Autorização para criação, alteração e eliminação de escalas de valores em domínio especificado;
- Autorização para criação, alteração e eliminação de informação de risco em domínio especificado;
- Autorização para manipulação dos períodos ativos de conceitos e atributos de risco.
- Autorização para criação, alteração e eliminação de relatórios de risco em domínio especificado;
- Autorização para criação, alteração e eliminação de relatórios de risco corporativo;
- Autorização para importação e exportação de informação de risco em domínio especificado.

R2.2.5. O SGRC deve permitir que um utilizador autorizado possa associar um ou mais papéis de utilizadores a um utilizador ou grupo de utilizadores.

2.3 Serviço de alertas de utilizadores

Um processo de gestão de risco é um processo que envolve uma constante monitorização e revisão da informação de risco de forma a garantir que a informação de risco está constantemente atualizada e relevante. De forma a simplificar a atividade de monitorização e revisão é necessário que o SGRC possua um serviço de alertas onde utilizadores são notificados de determinadas atividades provocadas por outros utilizadores tais como: novo objeto de risco, alteração de atributo de risco, eliminação de informação, entre outros.

R2.3.1. O SGRC deve permitir que um utilizador autorizador possa definir alertas de utilizadores com base na seguinte informação:
- Utilizador(es) ou grupo(s) de utilizador sobre o qual deseja receber alertas;
- Domínio(s) sobre o qual deseja receber alertas;
- Função(ões) ou evento(s) sobre o qual deseja receber alertas.

R2.3.2. Um alerta deve conter informação sobre:
- O utilizador que provocou o alerta;
- O domínio sobre o qual o alerta se refere;
- A função ou evento que provocou o alerta.

R2.3.3. O SGRC deve suportar um processo para notificar sobre a existência de alertas para um endereço de correio eletrónico.

2.4 Serviço de modelo de domínio

O contexto da gestão de risco na INCM é caracterizado pela existência de várias Estruturas de Gestão de Risco Especializadas. Cada estrutura pertence a um determinado contexto onde se encontra implementado um processo de gestão de risco. Um processo de gestão de risco especializado pode implicar diferentes conceitos, relações, terminologias e técnicas de risco.

R2.4.1. O SGRC deve permitir que um utilizador autorizado possa criar um domínio correspondente a uma estrutura de gestão de risco especializada com base na seguinte informação:
- Nome do domínio;
- Descrição do domínio;
- Privacidade (Publico ou Privado).

R2.4.2. O SGRC deve permitir que um utilizador autorizado possa alterar a informação identificada no requisito R2.4.1.

R2.4.3. O SGRC deve permitir que um utilizador autorizado possa desenhar um modelo de domínio através da implementação dos requisitos R2.4.4 a R2.4.5.

R2.4.4. O SGRC deve suportar um processo para criar, alterar e eliminar conceitos de risco.

R2.4.5. O SGRC deve suportar um processo para criar, alterar e eliminar relações entre conceitos de risco.

R2.4.6. O SGRC deve suportar um processo que permita definir a multiplicidade das relações entre conceitos de risco.

R2.4.7. O SGRC deve suportar um processo para associar atributos de risco a conceitos de risco.

R2.4.8. O SGRC deve suportar um processo para definir um atributo de risco como uma função que assume como argumentos outros atributos de risco relacionados.

R2.4.9. Sempre que a multiplicidade entre variáveis da função imposta pelo requisito R2.4.8. seja diferente de 1 para 1, o SGRC deve suportar um processo de ponderação de resultados.

R2.4.9. O SGRC deve suportar um processo para duplicar um modelo de domínio. A duplicação do modelo de domínio deve consistir na duplicação dos conceitos, relações e atributos de risco.

R2.4.10. O SGRC deve suportar um processo para eliminar um modelo de domínio.

2.5 Serviço de atributos de risco e escalas de valores

Um processo de gestão de risco envolve as atividades de análise e avaliação da informação de risco. Para tal assume-se que a informação de risco é caracterizada por um conjunto de atributos que permitem comparar e priorizar a informação. Os atributos de risco podem corresponder a escalas de valores qualitativas, quantitativas ou semi-qualitativas.

R2.5.1. O SGRC deve permitir que um utilizador autorizado possa criar um atributo de risco com base na seguinte informação:
- Nome do atributo;
- Obrigatoriedade do atributo (obrigatório ou opcional);
- Tipo do atributo.

R2.5.2. O SGRC deve permitir um utilizador autorizado possa alterar a informação identificada no requisito R2.5.1.

R2.5.3. O SGRC deve suportar, pelo menos, os seguintes tipos de atributo:
- Atributo textual;
- Atributo numérico;
- Atributo booleano;
- Atributo do tipo data;
- Escala de valores;

R2.5.4. O SGRC deve permitir que um utilizador autorizado possa eliminar um atributo de risco desde que este não esteja associado a um modelo de domínio.

R2.5.5. O SGRC deve permitir que um utilizador autorizado possa criar uma escala de valores com base na seguinte informação:
- Nome da escala de valores;
- Tipo da escala de valores;
- Privacidade da escala de valores (Publica ou Privada);

R2.5.6. O SGRC deve permitir um utilizador autorizado possa alterar a informação identificada no requisito R2.5.5.

R2.5.7. O SGRC deve suportar, pelo menos, os seguintes tipos de escala de valores:
- Qualitativo;
- Quantitativo;
- Tabela.

R2.5.8. O SGRC deve suportar um processo para criar escalas de valores qualitativas ordenáveis ou não-ordenáveis.

R2.5.9. O SGRC deve suportar um processo para criar escalas de valores quantitativas discretas ou continuas.

R2.5.10. O SGRC deve suportar um processo para criar escalas de valores do tipo tabela onde um utilizador autorizado pode definir:
- O número de atributos da escala de valores;
- O tipo dos atributos da escala de valores;
- Os valores dos atributos da escala de valores.

R2.5.11. Os tipos dos atributos da escala de valores suportados devem ser os mesmos do requisito R2.5.3.

R2.5.12. O SGRC deve suportar um processo para importar valores para uma escala de valores com base num ficheiro *Microsoft Excel* (*.xls* ou *.xlsx*).

R2.5.13. O SGRC deve permitir que um utilizador autorizado possa eliminar uma escala de valores desde que esta não esteja associada a um atributo de risco.

2.6 Serviço de registo de risco

Um processo de gestão de risco é suportado por um registo de risco - um objeto onde toda a informação de risco é registada. Mais concretamente, é uma ferramenta de suporte considerada essencial para a comunicação, consulta, monitorização e revisão dos riscos – os principais objetivos da gestão de risco corporativo.

R2.6.1. O SGRC deve permitir que um utilizador autorizado possa criar objetos de risco num determinado domínio de acordo com o respetivo modelo de domínio.

R2.6.2. O SGRC deve permitir que um utilizador autorizado possa alterar objetos de risco criados de acordo com o requisito R2.6.1.

R.2.6.3. O SGRC deve permitir que um utilizador autorizado possa remover objetos de risco criados de acordo com o requisito R2.6.1.

R2.6.4. O SGRC deve suportar um processo para visualizar em conjunto os objetos criados de acordo com o requisito R2.6.1.

R2.6.5. O SGRC deve suportar um processo para ocultar atributos de risco da visualização imposta pelo requisito R2.6.4.

R2.6.6. O SGRC deve suportar um processo para ordenar os atributos de risco da visualização imposta pelo requisito R2.6.4.

R2.6.7. O SGRC deve suportar um processo para filtrar a informação com base num termo de pesquisa da visualização imposta pelo requisito R2.6.4.

R2.6.8. O SGRC deve suportar um processo para importar e exportar objetos de risco para, pelo menos, um ficheiro *Microsoft Excel* (*.xls* ou *.xlsx*).

2.7 Serviço de planeamento e tempo

O contexto organizacional da INCM é caracterizado por mudanças constantes devido a novos requisitos internos, regulamentares ou legais. A dinâmica da organização resulta em recorrentes alterações do contexto onde a gestão de risco é implementada. A informação de como os riscos evoluem ao longo do tempo é relevante para a monitorização da gestão de risco, a sua eficácia e eficiência. Adicionalmente a gestão de risco resulta num conjunto de planos de tratamento de risco com o objetivo de alterar a exposição ao risco pela organização. A possibilidade de comparação do estado atual da organização no que diz respeito ao risco com o estado planeado é um instrumento de grande valor para a definição da estratégia da organização.

R2.7.1. O SGRC deve suportar um processo para gerir o período ativo de um objeto de risco.

R2.7.2. O SGRC deve suportar um processo para visualizar os períodos de atividade de um objeto de risco.

R2.7.3. O SGRC deve suportar um processo para gerir o período ativo de um valor de um atributo de risco.

R2.7.4. O SGRC deve suportar um processo para visualizar os períodos de atividade de um atributo de risco.

R2.7.5. O SGRC deve permitir que um utilizador autorizado possa definir o valor futuro de um atributo de risco.

R2.7.6. O SGRC deve permitir que um utilizador autorizado possa alterar o período de atividade de um objeto de risco.

R2.7.7. O SGRC deve permitir que um utilizador autorizado possa alterar o período de atividade de valor de um atributo de risco.

R2.7.8. O SGRC deve suportar um processo para visualizar a evolução dos objetos de risco e os seus respetivos atributos.

R2.7.9. O SGRC deve suportar um processo para comparar registo de riscos em diferentes períodos de tempo.

2.8 Serviço de pesquisa e relatórios de risco

Para garantir uma correta apreciação de riscos é necessário que a informação de risco seja sempre passível de ser encontrada por qualquer utilizador com permissões de acesso à mesma. Adicionalmente para garantir que as partes interessadas entendem e conseguem utilizar a informação de Risco, é essencial que todas as atividades de Risco envolvam a comunicação e consulta constante com essas partes. Neste contexto, a comunicação deve ser assegurada através da produção de **Relatórios de Risco**. Os Relatórios de Risco devem incluir toda a informação possível e necessária, estruturada e apresentada de acordo com as preocupações e necessidades do destinatário.

R2.8.1. O SGRC deve permitir que utilizadores encontrem, usando uma pesquisa, qualquer informação para a qual tenham permissões de acesso.

R2.8.2. O SGRC deve permitir que utilizadores restrinjam o resultado da pesquisa a um determinado conceito de risco.

R2.8.3. O SGRC deve permitir que utilizadores pesquisem apenas em atributos de risco selecionados.

R2.8.4. Quando pesquisando em texto livre o SGRC deve ordenar os resultados por relevância.

R2.8.5. O SGRC deve suportar um processo para combinar diferentes termos de pesquisa em diferente atributos ou conceitos de risco.

R2.8.6. O SGRC deve permitir que utilizadores restrinjam o resultado da pesquisa a um determinado período de atividade.

R2.8.7. O SGRC deve, por defeito, retornar apenas objetos de risco ativos nos resultados de uma pesquisa, a menos que o utilizador indique o contrário.

R2.8.8. O SGRC deve suportar um processo de exportação de resultados de pesquisa para, pelo menos, formato PDF.

R2.8.9. O SGRC deve suportar um processo de procura baseado em listas e dependências entre informação de risco.

R2.8.10. O SGRC deve suportar um processo para agrupar informação de um domínio de acordo com informação em comum.

R2.8.11. O SGRC deve suportar um processo para configurar relatórios de risco de um determinado domínio com base na seguinte informação:

- Nome do relatório;
- Tipo do relatório;
- Privacidade do relatório;

R2.8.12. O processo de configuração imposto pelo requisito R2.8.11. apenas deve permitir a configuração de relatórios passíveis de ser gerados no respetivo domínio.

R2.8.13. O processo de configuração imposto pelo requisito R2.8.11. deve suportar, pelo menos, os seguintes relatórios:

- Matrizes de risco contínuas ou discretas;
- Tabelas de risco ordenadas e/ou filtradas de acordo com preferência do utilizador.
- Comparação entre matrizes de risco ou informação de risco selecionada;
- Evolução temporal de informação de risco;
- Estatísticas de domínio.
- Grafos de dependência entre conceitos.

R2.8.14. O SGRC deve permitir que utilizadores autorizados executem relatórios de risco previamente configurados.

R2.8.15. O SGRC deve suportar um processo para visualizar relatórios de risco simultaneamente.

R2.8.16. O SGRC deve suportar um processo para exportar relatórios de risco para, pelo menos, formato *PDF*.

2.9 Serviço de risco corporativo

A Estrutura de Gestão de Risco Corporativos deve permitir oferecer num dado momento uma visão comum e transversal dos riscos operacionais e de negócio da organização com base na informação de risco gerada nas diversas Estruturas de Gestão de Risco Especializadas. A Estrutura de Gestão de Risco Corporativo tem como principal função informar o Conselho de Administração da INCM e como tal deve assegurar que a informação apresentada é sucinta e relevante. Portanto é necessário garantir que o registo de risco corporativo tem a capacidade de agregar riscos operacionais e de negócio sem restringir a possibilidade de analisar e avaliar a gestão de risco das diferentes Estruturas de Gestão de Risco Especializadas.

R2.9.1. O SGRC deve suportar um processo para agregação de registos de risco de diferentes domínios.

R2.9.2. O processo de agregação imposto pelo requisito R2.9.1. deve suportar, pelo menos, as seguintes funções de agregação:

- Agregação por valor máximo ou mínimo;
- Agregação por média;
- Agregação por ponderação;
- Agregação com base no melhor/pior cenário (por exemplo, 10 riscos mais ou menos severos).

R2.9.3. O processo de agregação imposto pelo requisito R2.9.1. deve suportar a criação de novo objeto de risco representativo da agregação.

R2.9.4. Aquando da criação de um objeto de risco representativo de agregação de acordo com o requisito R2.9.3., o SGRC deve assegurar a dependência do objeto aos riscos agregados.

R2.9.5. O SGRC deve suportar o serviço de pesquisa e relatórios de risco para o processo de agregação imposto pelo requisito R2.9.1.

Apêndice B

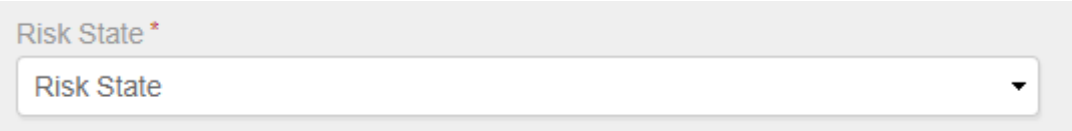


Figura 38 - Label de associação de enumerados

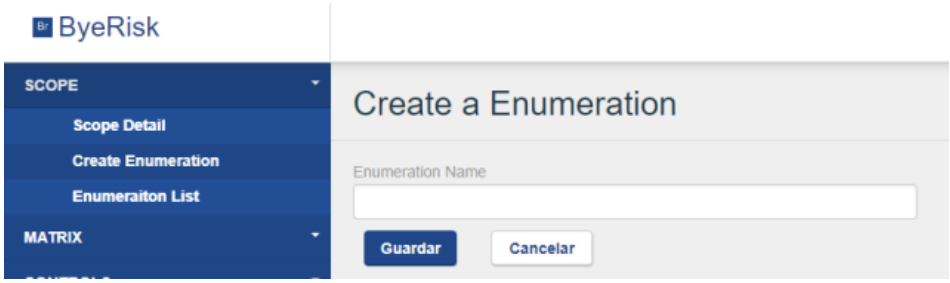


Figura 39 - Criação/Edição de um enumerado da aplicação

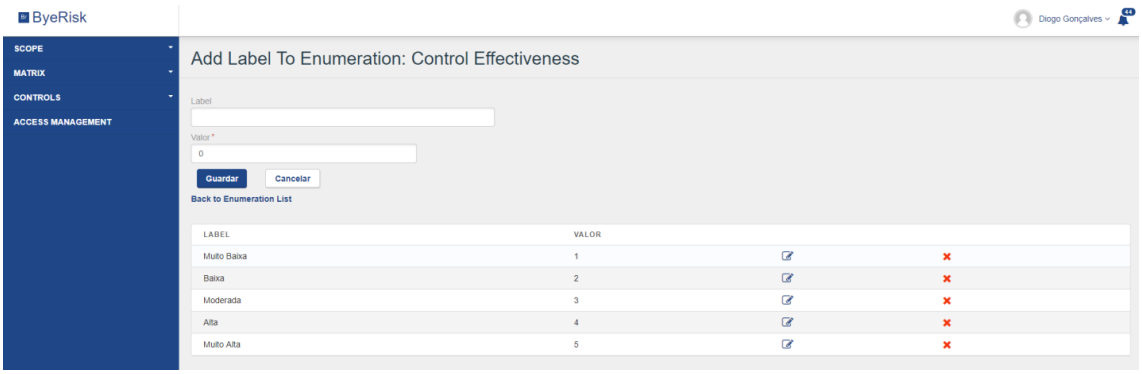


Figura 40 - Criação/Edição das labels de um Enumerado

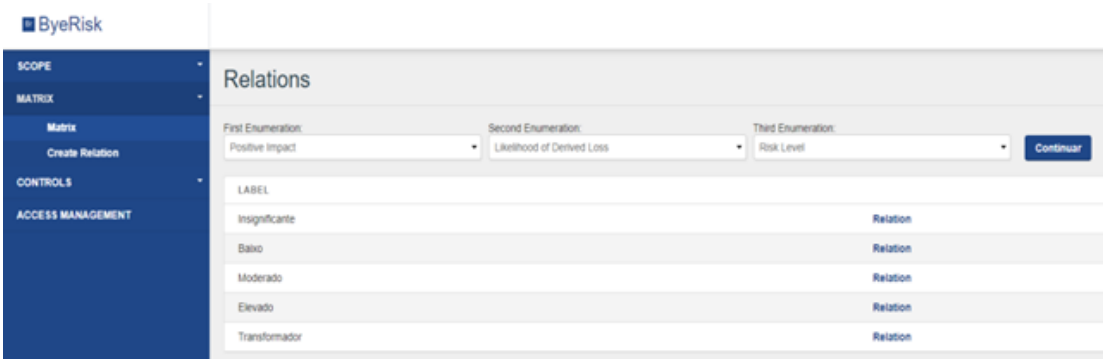


Figure 41 - Criação/Edição de relações

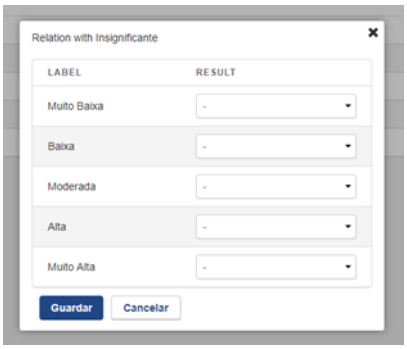


Figure 42 - Popup de criação/edição de relações

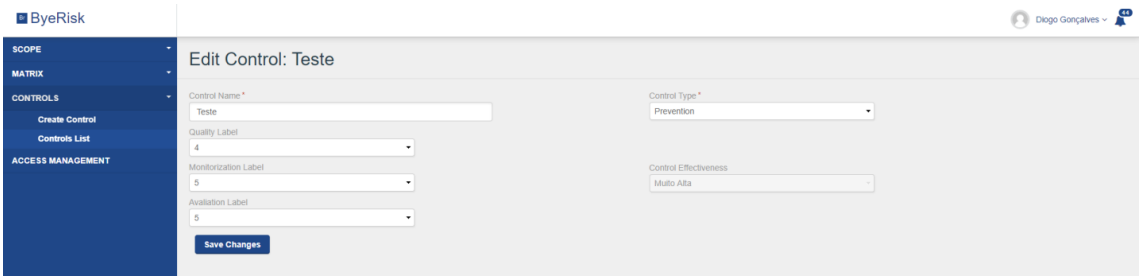


Figure 43 - Ecrã de edição de um controlo na aplicação

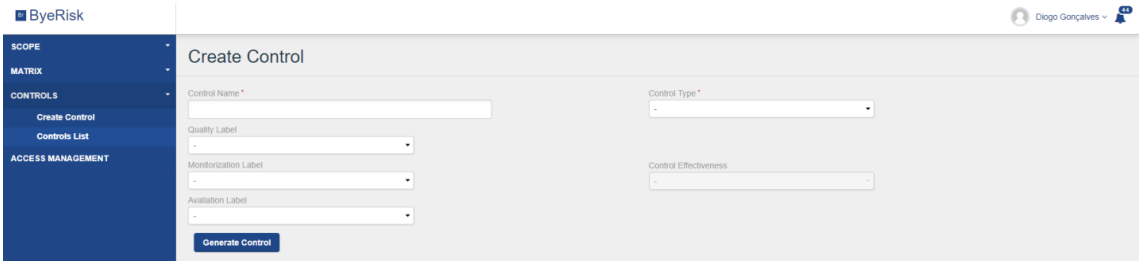


Figure 44 - Ecrã de criação de um controlo na aplicação

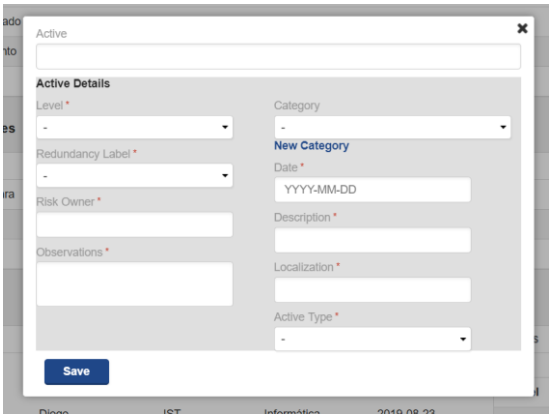


Figure 45 - Popup de criação/edição de um detalhe (Ativo)

Apêndice C

Objective	O01	Reputation	A01									
Objective	O02	Financial		A02								
Objective	O03	Quality			A03							
Asset	A01	Operationality of Kitchen Service	x	x	x			x				x	
Asset	A02	Operationality of Dining Room Service				x	x		x	x			
Asset	A03	Operationality of Home Delivery Service									x		
Risk Factor	**ID**	**Name**	**R01**	**R02**	**R03**	**R04**	**R05**	**R06**	**R07**	**R08**	**R09**	**R10**	**Scale**
Event	E01	Chef absent	x										Very Low
Event	E02	Assistant absent		x									Low
Event	E03	Trainee absent			x								High
Event	E04	Headmaster absent				x							Very Low
Event	E05	Waiter absent					x						Low
Event	E06	Kitchen is not operational						x					Very Low
Event	E07	Dinning room is not operational							x				Very Low
Event	E08	Motorcyle is not operational								x			Very Low
Event	E09	Home orders are not received									x		Low
Event	E11	Key ingredient not available										x	Medium
Consequence	Q01	Food cannot be produced	x					x					Very High
Consequence	Q02	Home delivery cannot be fulfilled					x			x			Very High
Consequence	Q03	Food cannot be served in a causeable time		x	x								Medium
Consequence	Q04	Food quality cannot be guaranteed										x	High
Consequence	Q05	Food cannot be served in house				x			x				Very High
Consequence	Q06	Costumers fill complaint of home delivery service									x		Very High
Control	C01	Assistant assumes chief role	C01										Very High
Control	C02	Trainee assumes assistant role		C01									Very High
Control	C03	Assistant makes extra time			C01								Very High
Control	C04	Waiter assumes headmaster role				C01							Very High
Control	C05	Trainnee assumes waiter role					C01						Very High
Control	C06	Headmaster informs affected costumers	Q01	Q03	Q03	Q05	Q02		Q06				Low
Control	C07	Home delivery by taxi								C02	C05		Very High
Control	C08	Key ingredient replaced by alternative										C04	Medium
Control	C09	Identify supplyer for emergencies										Q04	High
Control	C10	Disccount vouchers given to affected costumers						Q01		Q02	Q07		Low
Control	C11	Backup power generator						C03	C03				Medium
Cause	C01	Staff disease	x	x	x	x	x						
Cause	C02	Motorcycle is broken								x			
Cause	C03	Power outage						x	x				
Cause	C04	Faillure in stock management										x	
Cause	C05	Mobile phone network failure									x		