TÉCNICO LISBOA

Gestão de Risco na Continuidade de Negócio

João Pedro Cabral Teixeira

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática e de Computadores

Orientador: Prof. José Luís Brinquete Borbinha

Júri

Presidente: Prof. Luís Manuel Antunes Veiga
Orientador: Prof. José Luís Brinquete Borbinha
Vogal: Prof. Pedro Manuel Moreira Vaz Antunes de Sousa

Maio 2018

Agradecimentos

Ao Professor José Borbinha por toda a paciência que teve comigo ao longo deste trabalho e pela orientação que me deu.

À Associação DNS.PT por toda a ajuda, tempo e recursos que disponibilizaram para que eu pudesse concluir este trabalho.

Ao Tomás Martins por ser um irmão, um exemplo e o melhor amigo que eu alguma vez podia ter pedido.

À Rita Branco, por ser o meu porto seguro, por em todos os meus momentos de tristeza e de alegria me relembrar da beleza que há neste mundo.

Ao João Colaço de Freitas por todo a amizade, camaradagem e a orientação, pelo quanto me fez crescer como pessoa e como profissional.

À TMIST, pelas nossas noites de folia, canções, e pela familia que tive o prazer de passar a fazer parte.

À minha avó por toda a ternura e carinho que me deu ao longo da minha vida.

À minha irmã, por puder ver a mulher em que se está a tornar e o orgulho com que me enche.

À minha mãe e ao meu pai pelo amor, por tudo o que me ensinaram e por me terem dado a força para superar qualquer obstáculo e moldar o meu destino.

Ao meu avô, por me ter ensinado que a única pessoa que tem poder para moldar a minha vida sou eu.

E a todas as pessoas que tocaram a minha vida aos longo dos meus anos no Técnico por terem ajudado a moldar a pessoa que sou hoje.

Obrigado e até já.

Abstract

Uncertainty is everywhere, it is a dangerous condition to be in, not being able to foresee what the future may hold, or the consequences of action on the long term. But it can also be that some new and unforeseen opportunities may arouse from that uncertainty. Nonetheless, the risk is there, and companies, and any kind of organization, must make preparations so that they can best manage that uncertainty. Management Systems provide frameworks and processes so that organizations can better reach their goals and reduce the likelihood of any calamity or disaster.

These Management Systems directly affect the capacity that an organization has of enduring negative impacts and the amount of time and resources that it takes to recover, therefore, it is important that these Systems have appropriate technological support to back them up. With this project we propose to analyze the current risk management application implemented in Associação DNS.PT with the goal of understanding the overall business context on which it is used, identifying the other components from the organization that interact with it and provide a documented appreciation of the tool, which will point towards new developments. Having concluded these objectives, we were able to provide this specific organization with necessary documentation to further optimize and develop this application according to their requirements and needs.

Keywords: Management Systems, Risk, Business Continuity, Enterprise Risk Management.

Resumo

A incerteza está em toda parte, é uma condição perigosa para se estar, não sendo capaz de prever o que o futuro pode manter, ou as conseqüências da ação a longo prazo. Mas também pode ser que algumas oportunidades novas e imprevistas possam surgir dessa incerteza. Não obstante, o risco existe, e as empresas e qualquer tipo de organização devem fazer preparativos para que possam administrar melhor essa incerteza. Os sistemas de gerenciamento fornecem estruturas e processos para que as organizações possam alcançar melhor suas metas e reduzir a probabilidade de qualquer calamidade ou desastre. Estes sistemas de gestão afetam diretamente a capacidade que uma organização tem de suportar impactos negativos e a quantidade de tempo e recursos necessários para se recuperar, portanto, é importante que esses sistemas tenham suporte tecnológico apropriado para respaldá-los. Com este projecto propomos analisar a actual aplicação de gestão de risco implementada na Associação DNS.PT com o objectivo de compreender o contexto geral de negócio em que é utilizada, identificando os outros componentes da organização que interagem com ela e proporcionando uma apreciação documentada de a ferramenta, que apontará para novos desenvolvimentos. Tendo concluído esses objetivos, pudemos fornecer à organização específica a documentação necessária para otimizar e desenvolver ainda mais essa aplicação, de acordo com suas necessidades e necessidades.

Palavras-Chave: Sistemas de Gestão, Continuidade de Negócio, Gestão de Risco e Gestão de Risco Empresarial.

Lista de Tabelas

Lista de Figuras

Conteúdo

Capítulo 1

Introdução

1.1 Motivação

Qualquer organização, seja ela uma *startup* ou uma empresa multinacional, está exposta ao risco. Eventos inesperados como catástrofes naturais, perda de capital, lesões de colaboradores, entre outras, têm um profundo impacto negativo na organização o que pode levar à paragem das suas atividades ou até mesmo ao seu encerramento permanente. É imperativo que as organizações desenvolvam processos e ferramentas que assegurem as condições para não só suportarem esses evento mas também recuperar rapidamente dos danos causados. Esta necessidade que as organizações têm motiva o estudo do tema da Continuidade de Negócio,isto é, o desenvolvimento de métodos que permitem a um negócio continuar a funcionar dentro da normalidade e recuperar em caso de ocorrência de eventos prejudiciais.

Uma importante ferramenta e componente da Continuidade de Negócio é a Gestão de Risco, porque permite identificar de forma estruturada os eventos que produzem consequências disruptivas no negócio e ajuda a gerir e a prevenir adequadamente. A Gestão de Riscos ajuda as organizações a alcançarem os seus objetivos, pois sem a definição de procedimentos que indiquem quais as medidas a tomar face a acontecimentos malignos, a organização encontra-se-ia vulnerável à incerteza, aumentando a probabilidade de perder o seu rumo e não alcançe os seus objetivos.

O processo de identificar riscos, analisa-los, definir medidas e implementa-las é complexo, e pode tornar-se difícil de gerir se não houver um suporte adequado e que satisfaça as necessidades da organização.
Para que se possa maximizar o desempenho destes suportes, é necessário que exista um corretor alinhamento entre os vários componentes da organização envolvidas no processo, e isto só é possível se houver uma documentação adequada de todos os componentes. Isto permite não só transmitir confiança aos *stakeholders*, mas também facilitar a identificação de possíveis pontos de melhoria e de desalinhamento face aos objetivos estabelecidos.

Neste âmbito, realizou-se um estágio na Associação DNS.PT com o objetivo de análisar e implementar uma nova versão da aplicação informática que suporta o seu processo de gestão de risco.

1.2 Objetivos

Como foi referido anteriormente, o objetivo deste projeto é a análise e implementar uma nova versão da aplicação informática que suporta o processo de gestão de risco da Associação DNS.PT. Este trabalho tem como base os requisitos apresentados pela organização e as boas práticas definidas por referênciais internacionalmente reconhecidos. Esta nova versão da aplicação dará não só resposta aos *workflows* do processo de gestão de risco, mas também ser:

- Uma ferramenta de Gestão Documental, que auxilie os colaboradores da organização na realização das suas atividades;
- Um serviço remoto ao qual os colaboradores poderiam aceder de qualquer sitio;
- Um canal de envio e recepção de mensagens entre colaboradores, que permita alerta-los quando existir a necessidade de realizar determinadas tarefas.

A fim de contextualizar estes objetivos realizou-se uma análise para definir a abordagem a ser utilizada para desenvolver esta aplicação, no entanto, após se ter estudado mais a fundo o estado atual desta aplicação e os objetivos da Associação DNS.PT, determinou-se que o a fase de implementação do projeto era demasiado complexa e de maior duração do que o período estipulado para este projeto.

Assim sendo, redefiniu-se o âmbito e os objetivos passaram a ser:

- Analisar e identificar os componentes da Associação DNS.PT envolvidos no processo de gestão de risco a fim de contextualizar a aplicação informática;
- Estudar a aplicação informática e desenvolver para a organização um documento explicativo do seu estado atual, com propostas de possíveis melhorias.

Concluidos estes objetivos foi possível disponibilizar à Associação DNS.PT uma documentação que facilitará desenvolvimentos e melhorias futuras. Adicionalmente a documentação produzida sobre a estrutura e processos da organização servirão para a auxiliar a sua gestão diária caso seja necessário.

1.3 Estrutura do Documento

Neste capítulo foi realizada uma breve explicação das motivações que levaram à realização deste trabalho e quais os objetivos que se pretendem atingir. O resto do documento encontra estruturado em cinco capitulos:

- Capítulo 2: Será feito um levantamento do estado da arte nas temáticas de Continuidade de Negócio e de Gestão de Risco, assim como as normas ISO a elas associadas. Será ainda apresentado um estudo sobre o tema de Gestão de Risco Empresarial, com algumas das metodologias mais utilizadas;
- Capítulo 3: Pretende-se definir o contexto do problema apresentado e os passos que foram tomados desde a criação da aplicação informática até ao problema atual;
- Capítulo 4: É apresentado todo o trabalho realizado ao longo deste projeto, desde a análise e produção da documentação sobre a Associação DNS.PT e a aplicação até às propostas de melhoria identificadas;
- Capítulo 5: Por fim, será realizada uma reflexão sobre o trabalho realizado, o seu valor para a organização em questão e os progressos futuro que podem ser realizados sobre este projeto.

Capítulo 2

Trabalho Relacionado

Neste capítulo serão abordados os conceitos e temas usados ao longo do trabalho realizado. Os três principais conceitos deste projeto são os Sistemas de Gestão, a Continuidade de Negócio e a Gestão de Risco, com especial foco na última devido à sua relação com o processo suportado pela aplicação.

A aplicação análisada neste projeto está incluida no âmbito do sistema de gestão de risco da Associação DNS.PT. De forma a auxiliar a análise e o estudo desta aplicação é necessário compreender primeiro o que são os sistemas de gestão e como é que estes podem ser implementados e renovados dentro das organizações. Em seguida será aprofundada a implementação segundo os restantes âmbitos deste projeto, a Continuidade de Negócio e a Gestão de Risco, usando como referência as normas internacionalmente reconhecidas para a sua implementação nesses âmbitos. Finalmente este capítulo será concluido com a apresentação do conceito de Gestão de Risco Empresarial, ou *Enterprise Risk Management (ERM)*, que explora diferentes visões e práticas para implementação de uma estrutura de gestão de risco nas organizações.

2.1 Sistemas de Gestão

Nesta secção serão apresentados os conceitos referentes aos Sistemas de Gestão e às normas utilizadas para a sua implementação em organizações.

Os Sistemas de Gestão expandem-se por um grande leque de industrias e quando corretamente contextualizadas podem ajudar as organizações a tornarem-se mais competitivas na sua área. A Organização Internacional de Normalização (ISO), define um Sistema de Gestão como sendo *"...the way in which an organization manages the inter-related parts of its business in order to achieve its objectives"*[1]. As normas dos Sistemas de Gestão criadas pela ISO ajudam as organizações a melhorar o seu desempenho especificando um conjunto de passos que as organizações podem implementar para:

- Alcançarem os seus objetivos;
- Criarem uma cultura organizacional que constantemente se envolve num processo de auto-avaliação;
- Melhorarem constantemente através da consciêncialização dos seus colaboradores e liderança eficaz por parte da sua gestão de topo.

Os Sistemas de Gestão implementados segundo estas normas seguem a metodologia *Plan-Do-Check-Act*(PDCA) para o controlo e contínuo melhoramento dos seus produtos e processos. As principais

[1] `https://www.iso.org/management-system-standards.html`

funções de cada uma das atividades desta metodologia encontram-se representadas na Figura 2.1.

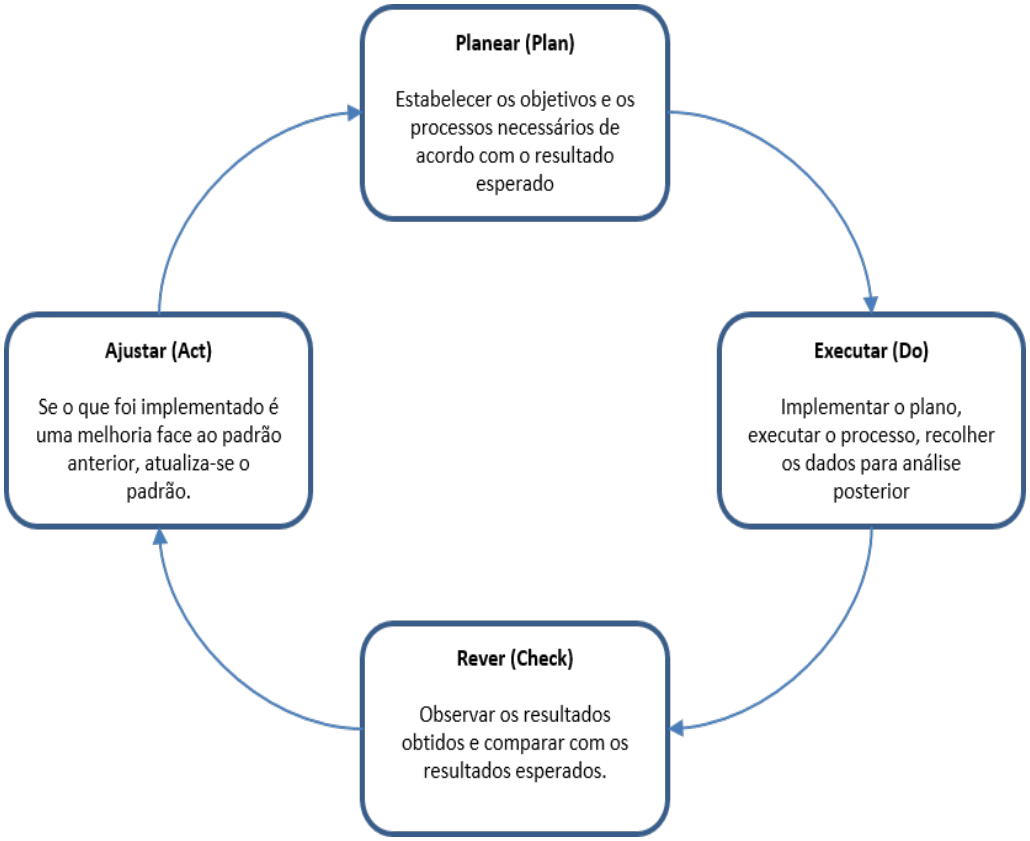

Figura 2.1: Metodologia *Plan-Do-Check-Act*.

As normas para a implementação de Sistemas de Gestão abordadas neste projeto são:

- ISO 9001:2015 *Quality Management Systems - Requirements*;
- ISO 22301:2012 *Societal security - Business continuity management systems — Requirements*;
- ISO 27001:2013 *Information Security Management Systems - Requirements*.

É importante destacar que a norma ISO 31000:2009 *Risk management - Principles and guidelines*, também será usada como referência ao longo desta projeto apesar de não definir requistos para a implementação de um sistema de gestão de risco, no entanto, *"...provides principles and generic guidelines on risk management."*[2], ou seja, define os principios e o vocabulário utilizado na gestão de risco, auxiliando assim a análise da aplicação da Associação DNS.PT.

Apesar de a Qualidade e da Segurança da Informação não serem as temâticas principais deste trabalho, foi a implementação dos seus Sistemas de Gestão que identificaram a necessidade de desenvolver um Sistema de Gestão de Risco. O contexto da implementação destes dois Sistemas de Gestão será elaborado mais detalhe no Capítulo 3 deste trabalho. A relação entre o Sistema de Gestão de Risco e

[2] `https://www.iso.org/standard/43170.html`

os Sistemas de Gestão para a Qualidade e para a Segurança de Informação implementados prende-se na relação que normas ISO utilizadas têm com o conceito do risco apresentado pela norma ISO 31000:2009:

- A revisão de 2015 da norma ISO 9001, veio acrescentar ao referencial uma dimensão de pensamento baseado em risco que já estava implicito em edições passadas da norma mas mais superficialmente através da realização de ações preventivas para eliminação de não conformidades.
- Na norma ISO 27001:2013 também é possível identificar na cláusula seis um planeamento que contempla a análise dos riscos identificados e o seu impacto nos objetivos para a segurança da informação.

2.2 Continuidade de Negócio

Nesta secção será feita uma descrição dos principais conceitos dentro da temática da Continuidade de Negócio assim como a norma ISO que define os requisitos para a implementação de um sistema de gestão para a Continuidade de Negócio.

A Continuidade de Negócio é definida como a *"capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident"*[2]. Estes eventos podem tomar a forma de desastres naturais, acidentes laborais, perda de suporte tecnológico, campanhas mediáticas negativas ou mesmo quedas vertiginosas na bolsa, entre outras. Por sua vez, a Gestão da Continuidade de Negócio é o processo holístico de gestão que *"...identifies potential threats to an organization and the impacts to business operations, those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation , brand and value creating activities"*[3] .

A norma ISO 22301:2012 é a referência internacional para a implementação de um sistema de gestão de continuidade de negócio e foi desenvolvido para ajudar as organizações a minimizarem o risco de eventos negativos. Especifica os requisitos para *"... plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise"*[3].As principais cláusulas da norma, onde se encontram especificados os requisitos para a sua implementação são:

- Cláusula 4 - Contexto da Organização;
- Cláusula 5 - Liderança;
- Cláusula 6 - Planeamento;
- Cláusula 7 - Suporte;
- Cláusula 8 - Operação;
- Cláusula 9 - Avaliação de Desempenho;
- Cláusula 10 - Melhoramento

Cláusula 4 - Contexto da Organização

A organização deve determinar e análisar os aspetos externos e internos que são relevantes para o seu próposito e que afetam a sua capacidade de atingir os objetivos do seu sistema de gestão de continuidade de negócio, tal como:

- As atividades, funções, serviços, produtos, as relações com os seus *stakeholders* e o potencial impacto de um evento disruptivo nelas;
- O alinhamento entre a política de continuidade, os objetivos da organização e outros princípios incluindo a sua estratégia de gestão de risco;
- O apetite de risco, ou seja, o nível de risco que uma organização está disposta a aceitar ao tentar alcançar os seus objetivos;
- As necessidades e expectativas das partes interessadas;
- As regulamentações, normas legais e outros requisitos que a organização se compromete a seguir.

Cláusula 5 - Liderança

A gestão de topo tem que demonstrar um compromisso constante com o sistema de gestão de continuidade de negócio para que seja possível criar um ambiente organizacional onde os diferentes atores desse sistema estejam inteiramente envolvidos, e onde então o sistema de gestão possa operar eficazmente em harmonia com os objetivos da organização. Esta gestão de topo é igualmente responsável por garantir que as responsabilidades e autoridades de pápeis chave são atribuídos.

Cláusula 6: Planeamento

A definição de objetivos estratégicos deve:

- Ser consistente com a política de continuidade de negócio;
- Ter em conta o nível mínimo de produtos e serviços que é aceitável para a organização atingir os seus objetivos;
- Ser mensurável;
- Ser monitorizado e atualizado à medida que for apropriado.

Cláusula 7 - Suporte

A gestão diária do sistema de gestão de continuidade de negócio é sustentada por uma utilização apropriada de recursos.
Cláusula 8 - Operação A operacionalização do sistema de gestão de continuidade de negócio inclui a utilização de cinco ferramentas:

- *Business Impact Analysis (BIA)*: O BIA é definido como o "...process of determining, assessing and evaluating the potential effects of an interruption or stoppage of critical operations, functions and processes of the business due to an accident, emergency, or disaster"[3];
- Avaliação de Risco: A norma ISO 22301:2012 usa a norma 310000 como referência para implementar o processo de gestão de risco;

- Estratégia de Continuidade de Negócio: Definição de medidas que permitirão à organização proteger e recuperar as atividades críticas para o seu negócio;
- Procedimentos de Continuidade de Negócio: A organização deve documentar procedimentos para assegurar que os objetivos da continuidade de negócio são atingidos. Estes procedimentos devem ser explicitos, flexíveis e criados tendo como base a análise de interdependências;
- Testes e Exercicios: Para garantir que os procedimentos são consistentes com os objetivos da continuidade de negócio estes devem ser testados regularmente.

Cláusula 9 - Avaliação de Desempenho e Cláusula 10 - Melhoramento

Após a implementação do sistema de gestão de continuidade de negócio, a norma ISO 22301:2012 requer que haja um processo de constante monitorização e revisão periodica para melhorar o seu desempenho, aumentar a eficácia e otimizar a eficiência.

2.3 Gestão do Risco

Nesta secção serão apresentados e abordados os conceitos relativos ao principal tema deste projeto: a Gestão de Risco. Será também descrita a norma ISO que define os principios para a definição de um processo de Gestão de Risco e discutida a temática de *Enterprise Risk Management*.

Como foi definido anteriomente, o efeito da incerteza sobre os objetivos e estratégias de uma organização é denomidado de ”risco”e por sua vez a Gestão de Risco é definida como *”...set of coordinated activities to direct and control an organization with regard to risk and whose main goal is to define prevention and control mechanisms to address the risk attached to specific activities and valuable assets.”*[4]. Finalmente, o desenvolvimento, implementação e continua melhoria de um sistema para a integração do processo de gestão de risco com os restantes processos de governância, estratégia e planeamento, permite desenvolver uma gestão de risco eficaz e alinhada com o contexto e objetivos estrátegicos da organização.

2.3.1 ISO 31000:2009 - Gestão de Risco

A norma ISO 31000:2009 tem como objetivo estabelecer normas, princípios e orientações para uma gestão de riscos eficaz e eficiente, que consequentemente ajuda as organizações a alcançarem os seus objetivos, melhorar a identificação de oportunidades ou ameaças, e melhorar a alocação e utilização de recursos para o tratamento de riscos.

Apesar de fornecer diretrizes e princípios gerais que as organizações podem utilizar, não é pretende promover uma gestão de risco uniforme. Os planos e estruturas de gestão de risco devem ser implementadas tenho em conta as necessidades especificas de cada organização. Por exemplo, quando implementada e gerida de acordo com esta norma, a gestão de risco permite a uma organização: [5]

- Aumentar a probabilidade de se atingir os objetivos;
- Encorajar uma gestão pro-ativa;
- Estar atenta para a necessidade de identificar e tratar os riscos ao longo de todas as camadas da mesma;

- Melhorar a confiança das partes interessadas;
- Melhorar os controlos;
- Minimizar perdas;
- Aumentar a resiliência.

O conjunto de princípos que estão na base da gestão de risco são: [5]

- Criar valor;
- Ser uma parte integrante dos processos organizacionais;
- Fazer parte da tomada de decisões;
- Abordar explicitamente a incerteza;
- Sistemática, estruturada e oportuna;
- Baseada em informações disponíveis;
- Feita à medida;
- Considerar fatores humanos e culturais;
- Transparente e inclusiva;
- Dinâmica, interativa e capaz de reagir a mudanças;
- Facilitar a melhoria continua da organização.

2.3.2 Processo de Gestão de Risco da norma ISO 31000:2009

O Processo de Gestão de Risco, definido pela norma ISO 31000:2009 encontra-se representado na Figura 2.2 contemplando as seguintes atividades: [5]

- Comunicação e Consulta;
- Estabelecimento do Contexto;
- Processo de avaliação de riscos
  - Identificação de riscos;
  - Análise de riscos;
  - Avaliação de riscos;
- Tratamento de riscos;
- Monitorização e análise crítica.

Comunicação e Consulta

Nem todas as entidades envolvidas numa organização ou num projeto percecionam o risco da mesma forma, devido a diferenças de valores, necessidades e preocupações, dessa forma é necessário que a comunicação com as partes interessadas seja realizada ao longo de todas as atividades do processo de gestão de risco.

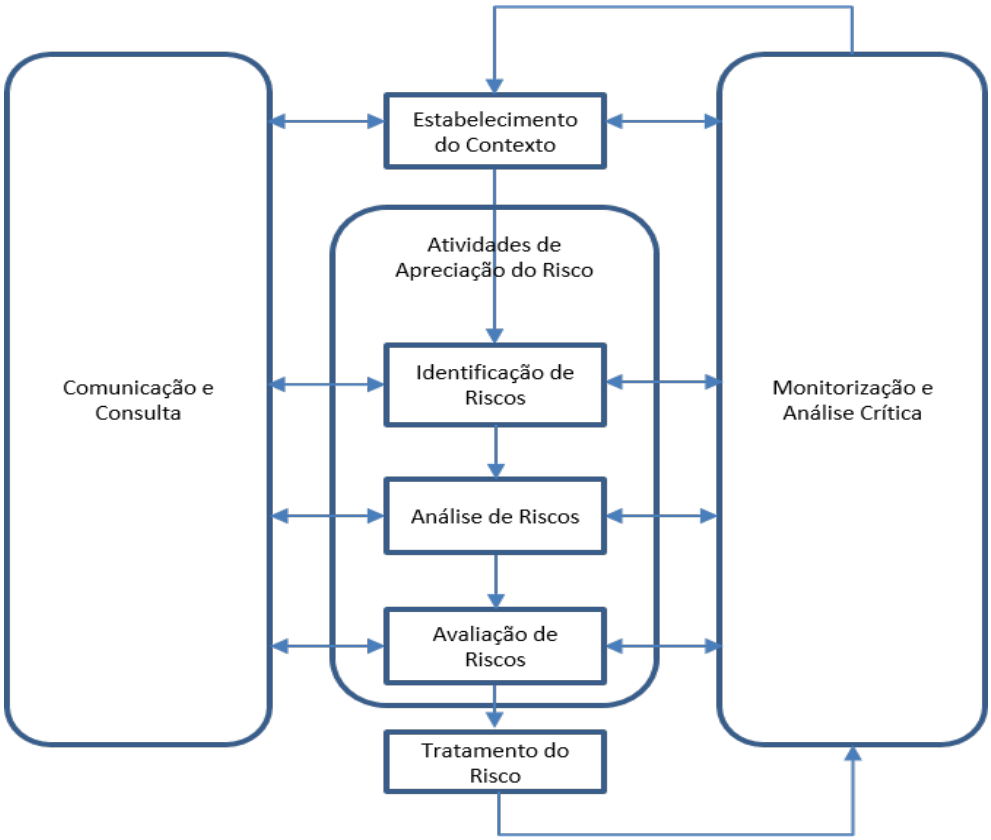

Figura 2.2: Modelo do Processo de Gestão de Risco da norma ISO 31000:2009.

A comunicação e consulta identifica, regista e tem em conta no processo de tomada de decisão, as várias perceções que as partes interessadas têm, uma vez que as suas opiniões têm um impacto significativo na tomada de decisão. Na tomada de decisão é importante que seja percetível para as partes interessadas quais as medidas de controlo de risco implementadas, por que razão são necessárias e que ações específicas terão de ser tomadas.

É importante que a comunicação e consulta facilite a troca de informações pertinentes, verdadeiras e compreensíveis, considerando a confidencialidade e integridade das pessoas.

Estabelecimento de Contexto

O estabelecimento do contexto permite a uma organização "...articulate their objetives, define the external and internal parameters to be taken into account in risk management and establish the scope and risk criteria for the remaining process"[5].

O contexto externo inclui fatores como ambientes culturais, sociais, políticos, legais, financeiros, tecnológicos e até mesmo as relações entre as partes interessadas. Por outro lado o contexto interno diz respeito a fatores como a governância, estrutura organizacional, funções e responsabilidades, a própria cultura da organização e os seus sistemas e fluxos de informação. Existem outros fatores que inflenciam o contexto de uma organização, tanto no interior como no exterior, e que devem ser tomados em conta para que seja possível estabelecer os objetivos, estratégias e os recursos que as atividades

usam, para além da definição das responsabilidades e autoridades necessárias.

É igualmente importante que a organização defina os critérios a serem utilizados para avaliar a importância do risco. e que estes estejam alinhados com a política de gestão de riscos da organização definidos no início do processo de gestão de risco e devem ser avaliados de uma forma critica e contínua. Alguns fatores que uma organização deve ter em conta aquando da definição dos critérios de risco são: [5]

- A natureza e os tipos de causas e consequências que podem occorer e como elas serão medidas;
- Como a probabilidade será definida;
- Como o nível de risco deve ser determinado;
- Os pontos de vista das partes interessadas;
- O nível em que o risco se torna aceitável ou tolerável;
- A combinação de múltiplos riscos e a sua consideração.

Processo de avaliação de Riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos. [5]

Identificação de Riscos

A identificação corresponde ao registo das fontes de risco, as áreas de impacto, os eventos, as suas causas e as suas consequências, no contexto dos objetivos da organização. É um passo crítico, porque um risco que não é identificado nesta fase pode ser excluído numa análise posterior. O resultado final desta fase corresponde a uma lista abrangente de riscos que envolva não só os riscos identificados em primeira ordem como sendo os mais obvios mas também as recações em cadeira que deles possam originar.

Análise de Riscos

A análise dos riscos consiste em retirar significado dos dados recolhidos anteriormente e definir as consequências negativas, ou impacto, dos riscos e a sua probabilidade. A combinação desses dois fatores determina o nível de risco, e fornece a informação necessária para a avaliação da necessidade dos riscos serem tratados e quais as estratégias e métodos mais eficientes.

Avaliação de Riscos

A avaliação dos riscos envolve o auxilio da tomada de decisão tendo em consideração os resultados da análise de risco, de quais os riscos é que necessitam de ser tratados e qual a prioridade que deve ser tomada no tratamento.

Tratamento de Riscos

O tratamento de riscos envolve a seleção de uma ou mais estratégias diferentes. que as organizações podem tomar relativamente à forma como lidam com os diferentes tipos de risco:

• **Eliminação:** Implementar ações para mitigar a incerteza o quanto possível, afim de evitar as consequências;

• **Aceitação:** Um risco é justificável de um ponto de vista comercializável e é decidido reter o risco e lidar com as possíveis consequências;

• **Transferência:** As consequências de um risco são partilhadas ou distribuídas entre os vários participantes do projeto ou através de terceiros;

• **Mitigação:** Reduzir o impacto que certos riscos podem ter nos seus processos da empresa através do ajuste de certos fatores.

As opções de tratamento de risco não são necessariamente mutuamente exclusivas ou adequadas em todas as situações sendo sempre necessário tentar equilibar de um lado os custos e esforços associadados e do outros os benefícios adquiridos. Ao selecionar a opção de tratamento de riscos, convém que a organização considere os valores e percepções das partes interessadas. No entanto, o tratamento dos riscos só por si pode introduzir novos riscos, devido ao fracasso ou ineficácia das medidas, isto exige que haja uma monitorização constante para garantir a eficácia.

Monitorização e Análise Crítica

A monitorização foca-se na melhoria constante do desempenho do processo de gestão de risco, através da documentação e registo da informação, com a finalidade de: [5]

- Garantir que os controlos sejam eficazes e eficientes no projeto e na operação;
- Obter informações adicinais para melhorar o processo de avaliação dos riscos;
- Analisar os eventos, mudanças, tendências, sucessos e fracasos e aprender com eles;
- Detetar mudnaças no contexto externo e interno, incluindo mudnaças nos critérios de risco e no prórpio risco, as quais podem requerer revisão dos tratamentos dos riscos e das suas prioridades;
- Identificaar os riscos emergentes.

2.4 Gestão de Risco Empresarial

Nesta secção será explorado o conceito de Gestão de Risco Empresarial, e algumas estruturas e práticas para a sua implementação.

2.4.1 Conceitos Fundamentais

A Gestão de Risco Empresarial, ou *Enterprise Risk Management (ERM)* é uma estrutura de gestão de risco, que surgiu do reconhecimento por parte de diversas entidades que os risco não deveriam ser geridos de uma forma isolada mas sim identificados, analizados, controlados dentro de uma única estrutura. As abordagens clássicas de gestão de risco, baseadas em experiências estatisticas não capturam todas as mudanças que podem existir nos mercados e na estrutura da própria organização. Na figura 2.3 podemos observar as principais diferenças entre estas duas abordagens[6].

O objetivo é juntar todas os componentes e sistemas e desenvolver um sistema de gestão de risco integrado, à escala de toda a organização e com estruturas dinâmicas para que se possa orientar não

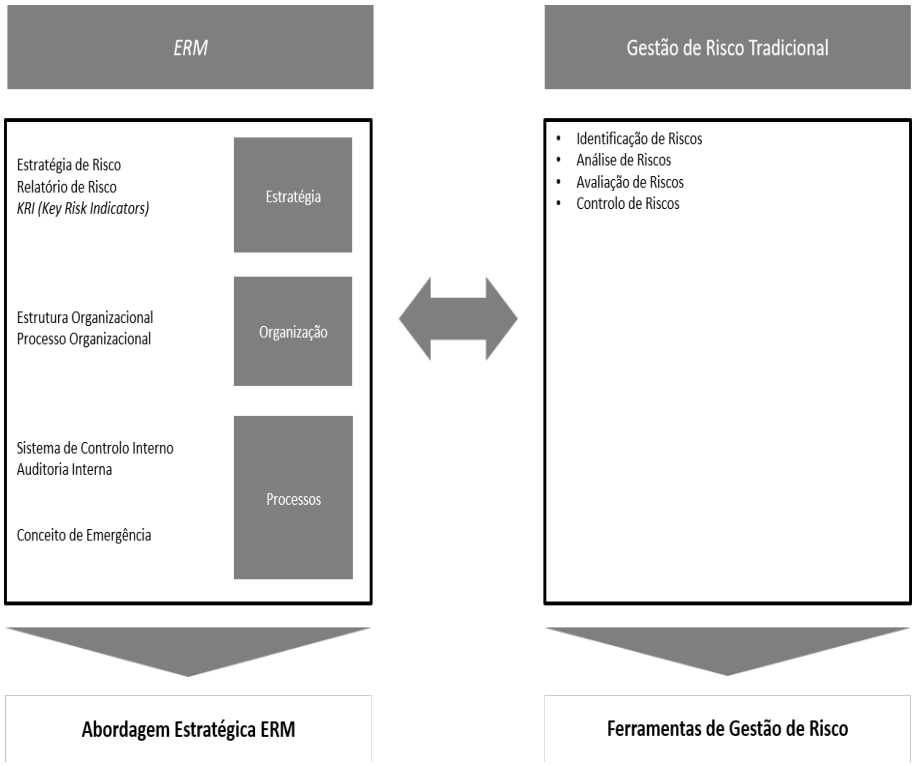

Figura 2.3: Comparação entre ERM e Gestão de Risco Operacional.

só aos objetivos mas também à estrátegia e à cultura da organização.

Atualmente, ainda não existe uma única estrutura definida, e reconhecida internacionalmente para *ERM*, no entanto, já existem algumas estruturas definidas que podem ser usadas como ponto de partida para a sua implementação. Nas próximas subsecções irão ser exploradas outras estruturas alternativas.

2.4.2 A Sociedade Aturial de Acidentes

A Sociedade Aturial de Acidentes ou *Casualty Actuarial Society (CAS)*, definiu *ERM* como ”the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization’s short- and long-term value to its stakeholders”[7].Esta abordagem ao *ERM* define *ERM* como sendo uma disciplina, um padrão ordenado de comportamento que tem o total apoio e compromisso da gestão da organização, o poder de influenciar tomadas de decisão e que acaba por se tornar uma parte da cultura da empresa.

Esta estrutura agrupa os tipos de risco da seguinte maneira:

- Desastre: Danos materiais, catástrofes naturais;
- Financeiro: Preço, ativos, moeda, liquidez;
- Operacional: Satisfação do cliente, falha do produto, integridade, risco de reputação, pobreza interna;
- Estratégico: Competição, capacidade de ativos, tendências sociais.

E os passos do processo de gestão de risco:

- Definição do Contexto: Compreensão das condições atuais em que a organização opera no contexto interno, externo e de gestão de riscos, são utilizadoas ferramentas como a análise *SWOT (Strength, Weakness, Opportunities, Threaths)*;

- Identificar os Riscos: Documentação das ameaças que afetem os objetivos da organização e a representação de áreas que a organização pode explorar para obter vantagem competitiva;

- Analisar e Quantificar os Riscos: Calibração e, se possível, criação de distribuições de probabilidade dos resultados para cada risco;

- Integrar os Riscos: Agregação de todas as distribuições de risco e a formulação dos resultados em termos do impacto nas principais métricas de desempenho da organização;

- Avaliar e Prioritizar os Riscos: Determinação da contribuição de cada risco para o perfil agregado de risco e priorização apropriada;

- Tratar e Explorar os Riscos: Desenvolvimento de estratégias para controlar e explorar os vários riscos;

- Monitorizar e Rever: Medição e monitorização contínuos do ambiente de risco e do desempenho das estratégias de gestão de risco.

2.4.3 Estrutura COSO para a Gestão de Risco Empresarial

O *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* define *ERM* como um "...process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[8].

Todas as organizações enfrentam incertezas, e o desafio para a gestão é determinar quanta incerteza suportar, ao mesmo tempo que se esforça para aumentar o valor das *stakeholders*. O retorno pelo investimento é maximizado quando a gestão define a estratégia e os objetivos para obter um equilíbrio ideal entre as metas de crescimento, retorno, riscos associados e implementa de uma maneira eficiente e eficaz os recursos para atingir os objetivos da organização.[8]

Esta estrutura apresenta o conceito de *ERM* segundo um conjunto de diretrizes:

- Uma reflexão da declaração de missão (cultura organizacional) da organização;

- Aplicável em sessões de estruturação de estrátegias;

- Aplicável em todos os níveis da organização;

- Capaz de produzir garantias para a gestão e para o comite de *stakeholders* sem retirar a responsabilidade do lado destes;

- Consegue oferecer uma categorização diversificada dos objetivos da organização

Esta estrutura de gestão de risco define uma matriz tridimensional onde incorpora em três dimensões as: categorias de risco, a estrutura hierarquica da organização e os componentes para uma gestão de risco eficaz. Os objetivos encontram-se divididos em quatro categorias para permitir o foco em diferentes aspetos da gestão de risco:

- Estrategia: Metas estratégicas de alto nível, alinhadas e apoiadas na missão da organização;
- Operações: Uso efetivo e eficiente dos seus recursos;
- Documentação;
- Conformidade com as leis e regulamentações aplicáveis.

Os componentes desta estrutura são:

- Contexto Interno: Define a forma como a organização conceptualiza o risco, e a filosofia que esta tem em relação ao risco;
- Definição de Objetivos: Garante que os seus objetivos suportam a missão da organização e o seu apetite de risco;
- Identificação de Eventos: Eventos internos e externos que afetem pelo positivo e pelo negativo a organização;
- Avaliação do Risco: Os riscos são avaliados com base no seu efeito inerente e residual;
- Resposta ao Risco: Desenvolvimento de um conjunto de acções para alinhar o nível dos riscos com o nível da tolerância da organização;
- Atividades de Controlo: Definição de políticas e procedimentos que ajudam a garantir que as respostas ao risco são realizadas;
- Comunicação e Informação: As informações relevantes são identificadas, capturadas e comunicadas de forma que permita às pessoas cumprirem as suas responsabilidades;
- Monitorização: Cumprida através dos processos de gestão e avaliação.

Estes oito componentes variam conforme o tamanho e o formalismo da organização. A *COSO ERM* é uma importante ferramenta na medida em que fornece uma abordagem atualizada sobre como uma organização pode gerir o risco e a incerteza, incorporando as diversas práticas e normas definidas, como a ISO 31000, e uma visão *top-down* de como aplicar o risco e expandi-lo a todos os elementos da organização.

2.4.4 Modelo de Maturidade de Risco - RIMS

A última estrutura *ERM* apresentada é o Modelo de Maturidade de Risco *RIMS*. Esta *framework* é definida como "...uma ferramenta de avaliação...para desenvolver e melhorar programas de gestão de risco empresarial sustentáveis"[1] permitindo às organizações avaliarem o seu processo de gestão de risco segundo um conjunto de indicadores e produzirem um relatório com pontos-chave para futuras melhorias(Figura 2.4).

Esta estrutura define motivadores de comportamento para a criação de uma estrutura *ERM* que permita criar valor e manter a integridade da organização. Os atributos que definem esta estrutura são:

- Gestão de processos focada;
- Gestão do apetite de risco da organização;
- Identificação eficiente de riscos;
- Gestão de desempenho;

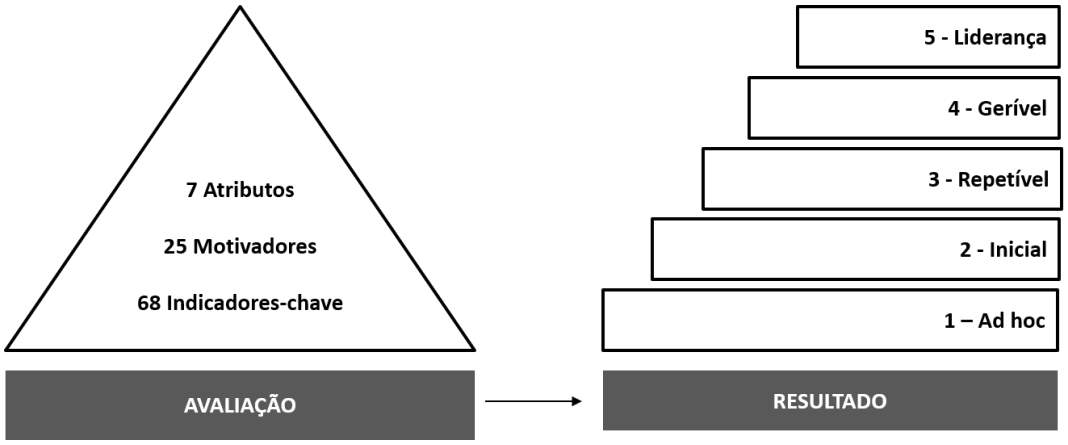

Figura 2.4: Modelo de Maturidade de Risco *RIMM*[1].

- Resiliência e sustentabilidade organizacional;
- Disciplina na procura do principal problema do processo.

Capítulo 3

Análise do Problema

Neste capítulo será descrito o contexto de onde este projeto surgiu, quais foram os desafios encontrados, e explicada a mudança de direção do projeto face ao que tinha sido inicialmente definido.

3.1 Contexto do Problema

Cada país tem um domínio de topo, um *Country Code Top-Level Domain* (ccTLD), que está reservado para esse país ou território nos termos do código ISO 3166-1. Cada ccTLD possui um *Registry*, que é a entidade responsável pela gestão, operação técnica e administrativa, e cuja delegação é efetuada pela *Internet Assigned Numbers Authority* (IANA). A IANA é a organização mundial que supervisiona a atribuição global dos números na Internet, entre os quais estão os números das portas, endereços IP, sistemas autónomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.

Enquanto *Registry* nacional a Associação DNS.PT, criada formalmente no dia 9 de Maio de 2013, tem como objetivo a gestão, operação e manutenção do registo do domínio de topo correspondente a Portugal(.PT) cumprindo, para o efeito a lei, os princípios da transparência e publicidade, os seus estatutos e as melhores recomendações nacionais e internacionais a nível técnico, administrativo e estratégico que lhe sejam aplicáveis.

A Associação DNS.PT apresenta um modelo associativo e *multi-stakeholder* de governação que lhe permite uma gestão mais eficiente, flexível e participativa dos diversos *stakeholders* que contribuem para a o crescimento do domínio de topo de Portugal. A organização tem como fundadores as as seguintes entidades:

- FCT.IP – Fundação para a Ciência e Tecnologia;
- ACEPI – Associação do Comércio Eletrónico e Publicidade Interativa;
- DECO – Associação Portuguesa para a Defesa do Consumidor;
- Um Representante designado pela IANA.

Do ponto de vista de prestação do serviço, existem dois tipos de clientes que interagem com o *Registry*, a Associação DNS.PT: os *Registrars* e os *Registrants*.

• ***Registrars*:** Entidade que compra um pacote de domínios ao *Registry*, para os incorporar enquanto produtos para disponibilizar para o consumidor final. O objetivo dos *Registry* para os *Registrars* é que estes lhes retirem a carga de trabalho de prestar suporte ao consumidor final, sendo que estas entidades possuem um certo nível de conhecimento técnico para o fazerem; [1]

•***Registrants*:** Consumidor final, individual ou coletivo, que procura adquirir um domínio para fins pessoais ou profissionais.[2]

Para além dos *Registrars* e dos *Registrants* a Associação DNS.PT também possui um serviço de Call-Center, através de *outsourcing* suportado pela organização Reditus que a ajuda a filtrar e a dar resposta aos pedidos dos seus clientes. Atualmente qualquer entidade pode comprar o seu domínio diretamente à Associação DNS.PT, fazendo com que esta adquira tanto a função de *Registry* como de *Registrar*.

Em 2013, a Associação DNS.PT iniciou a implementação de um sistema de gestão de qualidade como forma de responder às necessidades e exigências do seu negócio e garantir determinados níveis de eficiência e eficácia. A implementação do sistema de gestão de qualidade seguiu as diretrizes da norma ISO 9001:2008, sendo essa a norma ISO para sistemas de gestão de qualidade tomada como referência na altura. Mais tarde e face à natureza da sua função, a Associação DNS.PT iniciou em 2015 o processo de criação de um sistema de gestão da segurança de informação seguindo as referências definidas na norma ISO 27001:2013.

Na implementação da norma ISO 27001:2013, e segundo o controlo A.17 constante do Anexo A da norma, surgiu a necessidade de desenvolver o tema da Continuidade de Negócio. Neste âmbito foi acolhido um estágio de mestrado, em 2016, que desenvolveu tema de ”Processo de Gestão de Risco para Segurança da Informação e Continuidade de Negócio”da qual resultou a metodologia do processo de gestão de risco e continuidade de negócio.[9].

Posteriormente, a introdução do tópico da gestão de risco no negócio veio a ser reforçada pela nova versão da ISO 9001:2015 com uma abordagem que destaca mais o risco que as suas versões anteriores. Assim sendo, para suportar o sistema de gestão da segurança de informação a Associação DNS.PT criou uma estrutura de gestão de risco em conformidade com a norma ISO 31000:2009, e com o respetivo suporte tecnológico necessário, tendo esta sido mais tarde expandida para abrangir os restantes sistemas de gestão mencionados até agora.

Atualmente a aplicação informática encontra-se alinhada com os seguintes referênciais e normas:

- ISO 9001:2015 – Sistema de Gestão de Qualidade;
- ISO 27001:2013 – Sistema de Gestão da Segurança de Informação;
- ISO 22301:2012 – Sistema de Gestão da Continuidade de Negócio;
- ISO 31000:2009 – Gestão de Risco;
- Regulamento Geral da Proteção de Dados, 2016/679 de 27 de abril de 2016.

Atualmente, face às exigências do negócio e das suas partes interessadas, a Associação DNS.PT decidiu analisar e melhorar a ferramenta tecnológica desenvolvida sobre a ferramenta Microsoft Access, ao mesmo tempo que garantem um correto alinhamento entre o seu suporte tecnológico e a legislação

[1] `https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en`
[2] `https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en`

aplicável.

De forma a contextualização da aplicação, procedeu-se à análise de toda a arquitetura da organização incluindo os seus processos, aplicações e tecnológias. Esta etapa do trabalho foi realizada com o auxílio da nomenclatura Archimate, e da ferramenta Archi, e permitiu modelar a organização segundo as camadas de: Negócio, Aplicação e Tecnológia. Os objetos da linguagem utilizada foram:

- **Camada de Negócio** :
  - Ator de Negócio: Entidade capaz de realizar determinados comportamentos;
  - Papel de Negócio: Responsabilidade por realizar comportamentos específicos, aos quais um ator pode ser designado, ou a parte que um ator desempenha numa determinada ação ou evento;
  - Processo de Negócio: Sequência de comportamentos de negócio que alcançam um resultado específico, como um conjunto definido de produtos ou serviços de negócio;
  - Serviço de Negócio: Comportamento de negócio explicitamente exposto;
  - Objeto de Negócio: Conceito usado num domínio de negócio específico;
  - Interface de Negócio: Ponto de acesso onde um serviço de negócios é disponibilizado para o contexto da organização.
- **Camada de Aplicação** :
  - Componente da Aplicação: representa um encapsulamento da funcionalidade da aplicação. Encapsula o comportamento e dados, expõe os serviços e disponibiliza-os através de interfaces;
  - Serviço de Aplicação: Especifica como a funcionalidade de um componente pode ser acedida por outros elementos;
  - Interface de Aplicação: Expõe os serviços de aplicatição ao ambiente. O mesmo serviço de aplicação pode ser exposto por meio de diferentes interfaces e a mesma interface pode expor vários serviços.
- **Camada de Tecnologia** :
  - Dispositivo: É um recurso tecnológico físico sobre o qual o software do sistema e os restantes artefatos podem ser armazenados ou instalados para execução;
  - Sistema de Software: Software que fornece ou contribui para um ambiente de armazenamento, execução e uso de software ou dos dados instalados dentro dele;
  - Serviço Tecnologico: Serviço que explicitamente define o comportamento da tecnologia.

Começou-se por definir e representar o contexto externo e interno da Associação DNS.PT, as entidades presentes e as relações que estas têm com a organização.
O contexto externo diz respeito ao ambiente legal, regulatório, económico, natural e competitivo em que a organização se insere, e onde é possível definir os motivadores externos. A Associação DNS.PT possui um contexto externo relativamente simples (Figura 3.1), tendo como principais *stakeholders*, as entidades fundadoras, e tipos bastante bem definidos de clientes.

Para que a Associação DNS.PT seja capaz de prestar os seus serviços aos clientes é necessário que existam plataformas que possibilitem a comunicação bilateral entre as duas entidades. As Interfaces de Negócio através das quais a organização disponibiliza os seus Serviços de Negócio encontram-se representadas na Figura 3.2. A Associação DNS.PT disponibiliza três tipos de serviços aos seus clientes:

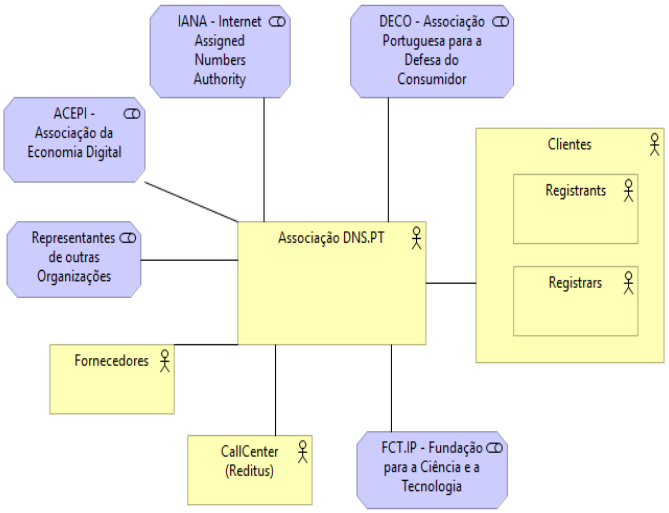

Figura 3.1: Diagrama de Contexto Externo da Associação DNS.PT.

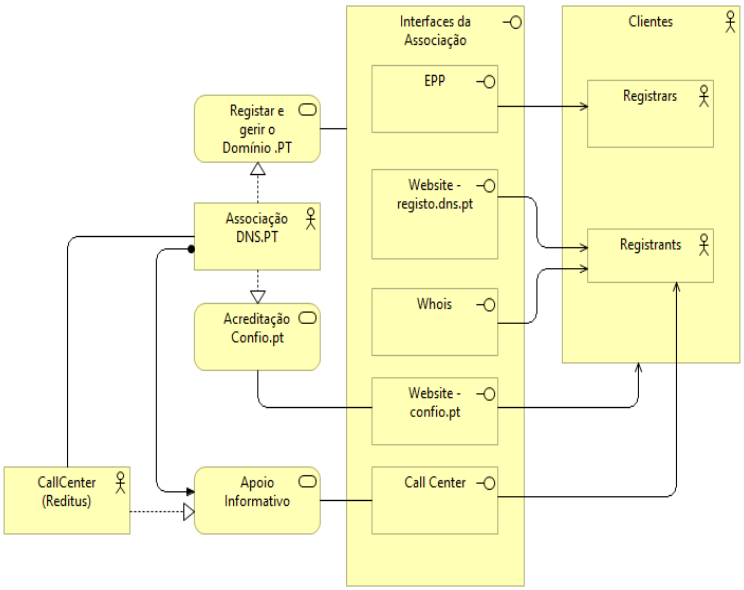

Figura 3.2: Serviços de Negócios da Associação DNS.PT.

- Registo e Gestão dos Domínios .PT: Os clientes podem adquirir dominios efectuando uma compra junto das entidades especializadas nas suas vendas (*Registrars*), ou comunicar diretamente com a Associação DNS.PT;
- Acreditação Confio.pt: Permite aos clientes adquirirem um selo de garantia de segurança para os seus domínios;
- Apoio informático: Suportado em parte pelo serviço de outsourcing conferido ao CallCenter, que permite aos clientes colocarem perguntas ou sulicitarem ajudas sobre problemas relativos aos seus domínios.

Relativamente ao Contexto Interno da Associação DNS.PT, este apresenta uma estrutura hierarquica organizada por áreas tal como foi referido no capítulo 3:

• **Conselho Diretivo:** Aprovação dos principais instrumentos de gestão e orientação geral da atividade da organização;

• **Assessoria, Comunicação e Relações Internacionais:** Acompanhamento das matérias de índole jurídica que decorram das atividades da associação, para além da produção de conteúdos de divulgação da atividade e gestão de iniciativas, participações a nível nacional e internacional;

• **Direção de infraestruturas e sistemas:** Coordenação e direção das atividades técnicas, planeamento e controlo dos diversos projetos técnicos;

• **Direção de Gestão e Administração:** Planeamento e gestão de toda a atividade administrativa relativa ao registo e manutenção de domínios .PT. Gestão da vertente contabilistíca e financeira e das restantes atividades de suporte: Recursos Humanos, secretariado e Gestão da Qualidade;

• **Responsável Segurança da Informação:** Planeamento, Controlo e Monitorização no âmbito da Segurança de Informação;

• **Secretariado:** Apoio logístico e administrativo.

Estas por sua vez contêm áreas mais especializados com um conjunto de funções e responsabilidades mais especificas (Figura 3.3). A definição e atribuição destas funções é essencial para que seja possível definir as competências necessárias para desempenhar os processos de negócio. A

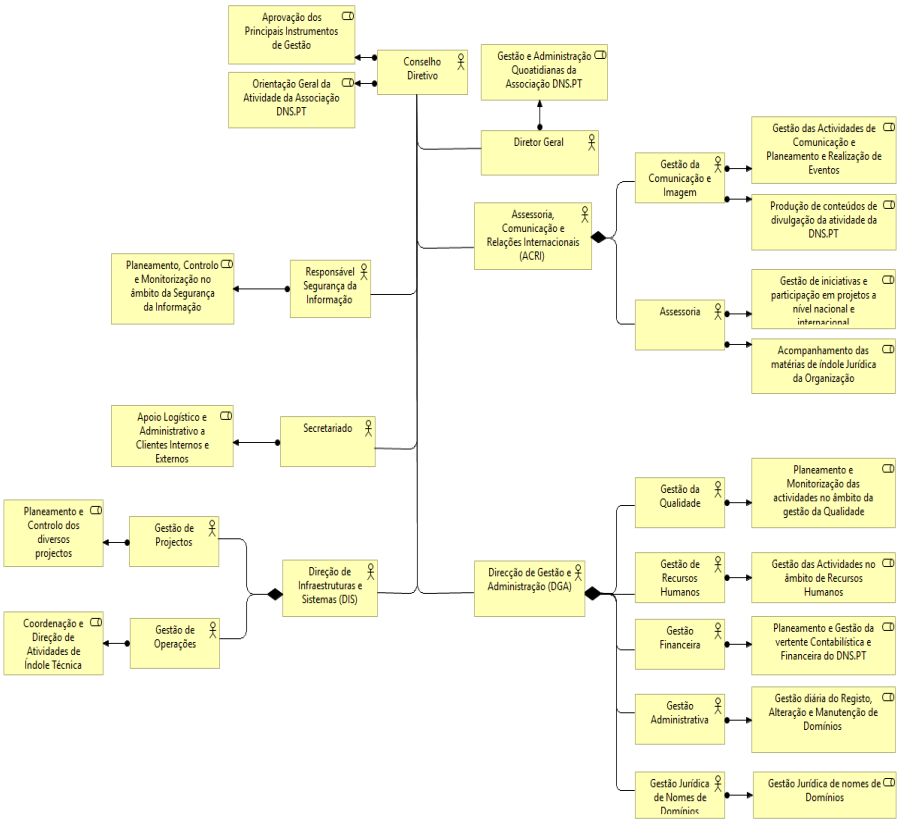

Figura 3.3: Diagrama do Contexto Interno da Associação DNS.PT.

organização apresenta uma estrutura hieraquica de processos, especificando processos mais concretos dentro de processos de negócio denominados MacroProcessos. A listagem destes Processos de Negócio encontra-se representada na Tabela B.1 no Anexo B.1.

O Processo de Negócio relativo à gestão de risco é o ”FP.02 Gerir e Tratar o Risco”, encontra-se englobado dentro do MacroProcesso ”MP.01 Planear e Melhorar a Organização e Segurança de Informação”. Este Processo de Negócio visa estabelecer a metodologia de avaliação e gestão de risco que coloque em causa a confidencialidade, integridade e disponibilidade dos artefatos associados às atividades da Associação DNS.PT.

O Processo de Negócio FP.02 tem os seguintes *inputs* e *output*:

- *Inputs*
  - Indicadores de desempenho;
  - Objetivos da organização;
  - Não conformidades identificadas e tratadas
  - Registos armazenados;
  - Resultados de auditorias;
  - Matriz de Análise de Risco;
  - Necessidades de Segurança de Informação
- *Outputs*
  - Relatório de Análise de Risco
  - Plano de Tratamento de riscos;
  - Declaração de Aplicabilidade.

Para todos os processos, procedeu-se em seguida à identificação de quais as entidades que os suportam, ou seja, quais as aplicações que encapsulam o comportamento necessário para que o Processo de Negócio possa ser realizado. Estas aplicações, denominadas por ”Sistemas de Informação”, no contexto da Associação DNS.PT, foram modelados utilizando a nomenclatura do Archimate como Componentes de Aplicação. Esta informação foi extrapolada de um relatório BIA fornecido pela organização e onde se encontravam especificados todos os diferentes Processos de Negócio e os ”Sistemas de Informação”a eles associados.Para este propósito foi desenvolvida uma lista com todos os ”Sistemas de Informação”usados pela organização (Anexo B.2) assim como representações da comunicação desta camada com a camada de negócio.

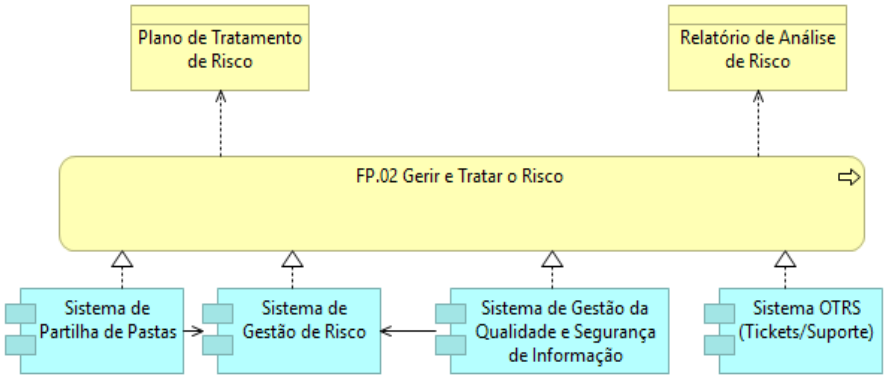

Figura 3.4: Comunicação ente as Camadas de Negócio e de Aplicação do Processo de Negócio FP.02

Os Componentes de Aplicação que suportam o Processo de Negócio FP.02 são (Figura 3.5):

- Sistema de Partilha de Pastas: Suporte à partilha de informação entre os colaboradores da organização numa área interna partilhada, para a qual é necessário credênciais de autenticação para aceder;
- Sistema de Gestão de Risco: Suporte ao processo de gestão de risco, através da gestão de informação;
- Sistema de Gestão de Qualidade e de Segurança de Informação (SGQSI)]: Sistema que armazena as representações BPMN relativas dos Processos de Negócio da organização, com os seus respectivos *workflows*, atividades e atores. Este sistema permite auxiliar tanto a realização diária de tarefas como a revisão do atual estado do negócio;
- Sistema OTRS (Tickets/Suporte): Sistema de captação de *tickets* para resolução de dificuldades que os *Registrars* ou *Registrants* possam ter. Estes textitTickets são recebidos e captados pelo Sistema de Email.

No projeto de estágio realizado no anterior pelo aluno João Fialho [9], foi desenvolvido um Diagrama BPMN onde foi representado o fluxo e as atividades intrísecas do processo de negócio FP.02, que serão exploradas em detalhe na secção seguinte. No contexto da Assoicação DNS.PT este diagrama encontra-se inserido dentro do âmbito do ”Sistema de Gestão de Qualidade e de Segurança de Informação (SGQSI)”e foi redesenhado para a organização. Esta representação pode ser observada na Figura 3.5.

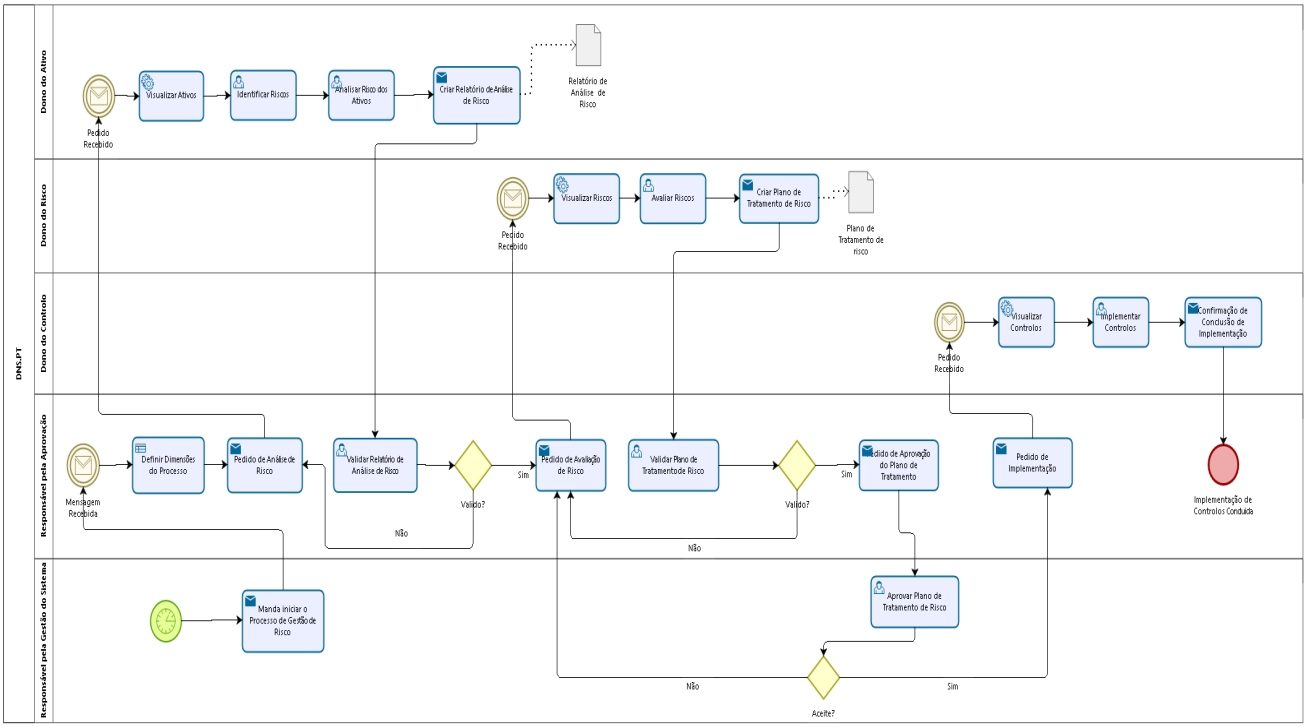

Figura 3.5: Diagrama BPMN - Processo de Negócio FP.02 Gerir e Tratar o Risco.

Finalmente, foram análisadas as tecnologias que suportam os Sistemas de Informação da secção anterior. Os dispositivos tecnológicos utilizados da Associação DNS.PT dividem-se por duas localizaçõess: A sede da DNS.PT e o Datacenter. A distribuição dos Dispositivos por estas áreas encontra-se representada na Figura 3.6.

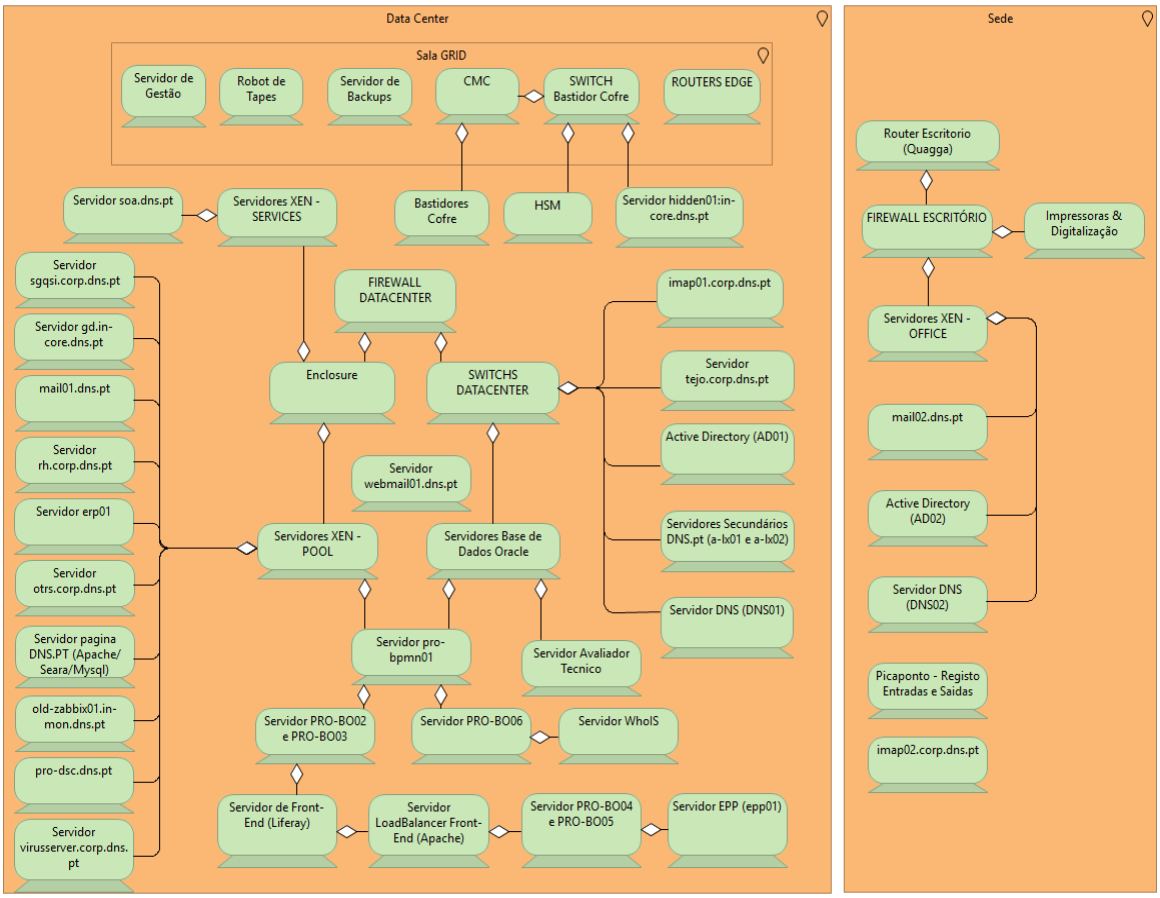

Figura 3.6: Dispositivos da Associação DNS.PT

Os Dispositivos implementam os Sistemas de Softwares (Lista em Anexo B.3) , e estes disponibilizam Serviços Tecnológicos para os Sistemas de Informação da Camada de Aplicação. Na Figura 3.7 encontra-se representado os Serviços, Softwares e Dispositivos Tecnológicos que suportam os Sistemas de Informação do Processo de Negócio FP.02.

Desde o início da análise à organização da Associação DNS.PT que o principal objetivo era adquirir uma visão geral das entidades envolvidas em todo o processo de gestão de risco. Ao usar a linguagem Archimate e a ferramenta Archi foi possível representar as várias entidades sobre as três camadas definidas. Graças a este projeto é possível visualizar para qualquer entidade da organização as relações e dependências que esta tem, o que permite assegurar que a Associação DNS.PT tem a capacidade de perceber rapidamente o impacto que cada mudança pode ter na organização. A Figura 3.8 mostra todos as entidades da Associação DNS.PT envolvidos no processo de gestão de risco FP.02.

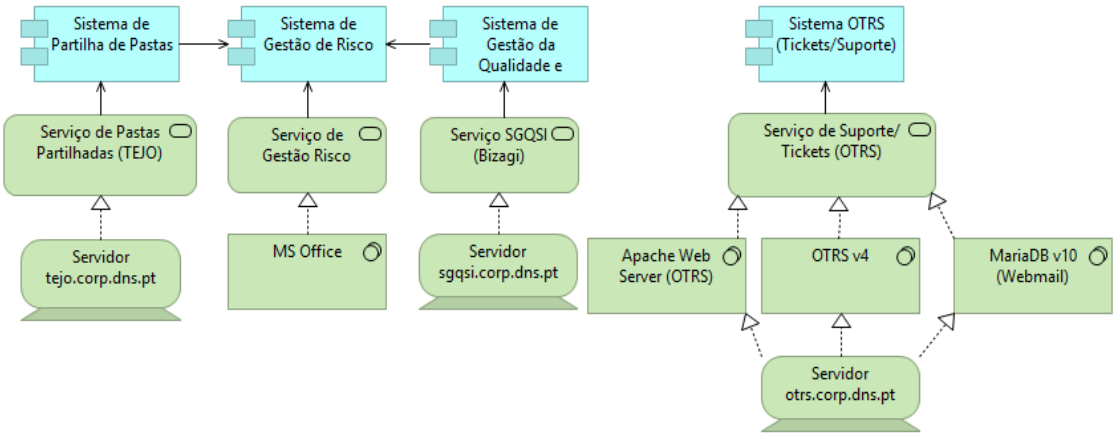

Figura 3.7: Componentes da Camada Tecnologica que suportam o Processo de Negócio FP.02

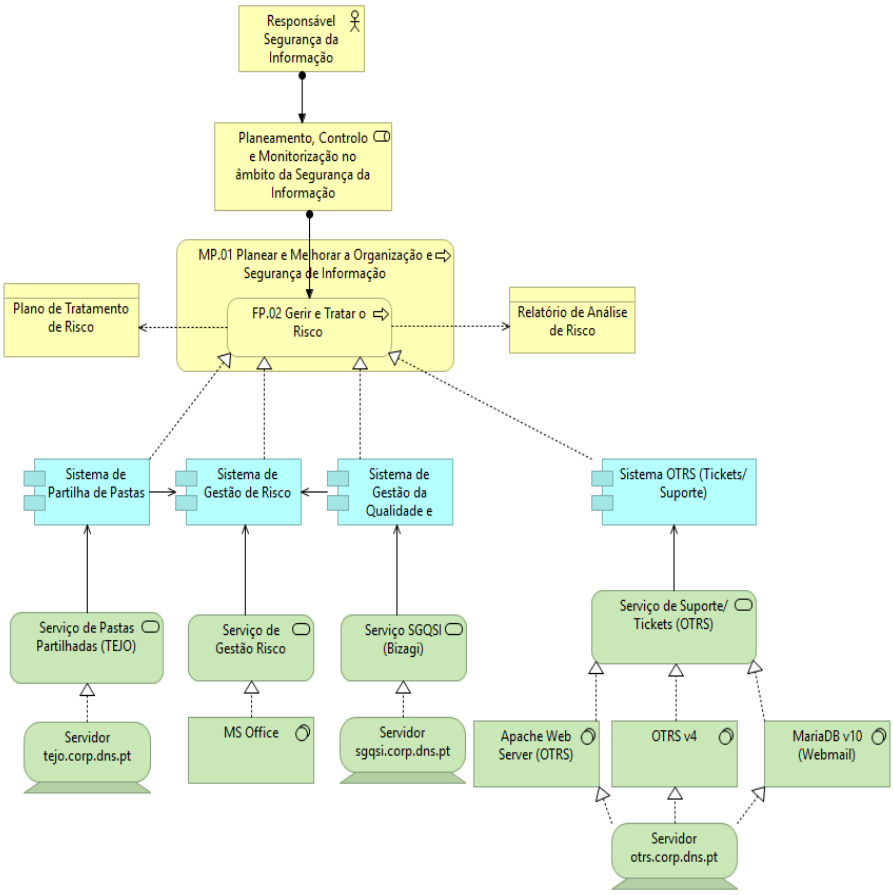

Figura 3.8: Entidades envolvidas no Processo de Gestão de Risco da Associação DNS.PT.

3.2 Análise da Aplicação Informática

Nesta secção será explorados três perspetivas diferentes sobre a aplicação informática que suporta o processo de gestão de risco da Associação DNS.PT. Irá ser análisado o modelo de dados e as entidades deste que são a base da arquitetura do sistema. Serão identificadas as funcionalidades disponibilizadas atualmente pela aplicação e finalmente, uma descrição da utilização da aplicação do ponto de vista do

utilizador.

3.2.1 Modelo de Dados

Nesta subsecção será análisado o modelo de dados da aplicação informática identificando os principais conceitos e relações. Nesta fase da análise o primeiro passo foi extrair o modelo de dados do Microsoft Access, e redesenha-lo, uma vez que o modelo retirado na sua forma crua tornava a compreensão complicada (Figura A.1, Anexo A).

Para este efeito foi escolhida a ferramenta Enterprise Architect para representar o modelo e tornar a visualização mais simples, ao mesmo tempo que se manteve a integridade dos atributos. A versão do modelo refeito encontra-se na Figura 3.9. Anteriormente à análise deste modelo, as reuniões com os

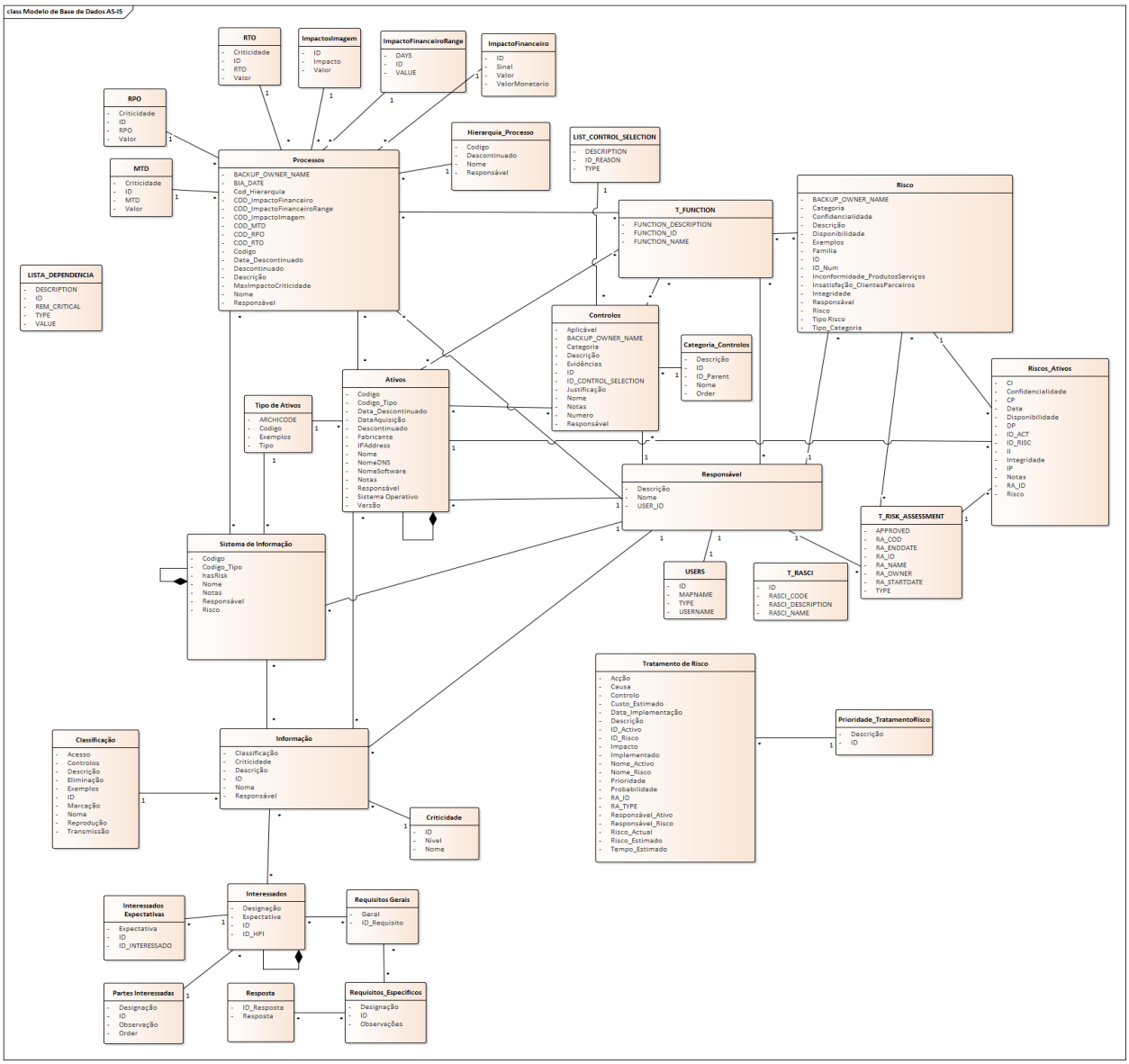

Figura 3.9: Modelo de Dados da Aplicação Informática Modelado em Enterprise Architect.

colaboradores da Associação DNS.PT, já tinham dado a entender que no núcleo deste processo existia um conjunto de entidades essenciais para o seu funcionamento. Estas entidades do modelo e as suas

respetivas definições foram:

- **Ativo:** Recursos que sustentam a informação e negócio da Associação DNS.PT, incluindo, dados em papel e em formato digital, processos, pessoas e tecnologias;

- **Informação:** Não apenas suporte eletrónico (bases de dados, arquivos em PDF, Word, Excel, e outros formatos), mas também em papel;

- **Sistema de Informação:** Conjunto de ativos que interagem entre si para produzir um produto ou fornecer um serviço;

- **Processo:** Conjunto de atividades estruturadas que têm como resultado final a prestação de serviço ou produto uniforme;

- **Risco:** O Efeito da incerteza nos objetivos;

- **Controlo:** Medida tomada contra um risco, que pode ser através de: eliminação, transferência, mitigação ou aceitação do risco, não sendo estes mutuamente exlusivos;

- **Responsável:** A entidade ”Responsável”, corresponde a um utilizador a quem lhes foi associado um ou mais artefactos (Ativos, Processos, Riscos, Controlos, Informação e Sistema de Informação). Esse utilizador deve realizar as suas funções, de analisar, avaliar, implementar ou validar mediante o tipo de artefactos e responsabilidades que detêm.

Na secção seguinte serão demonstrado, sob a forma de diagramas de Casos de Uso UML, as funcionalidades disponibilizadas pela aplicação informática, do ponto de vista de funcionalidade.

3.2.2 Casos de Uso

Nesta secção serão apresentados os Casos de Uso que identificam as principais funcionalidades fornecidas pela aplicação, e quais os atores que as realizam. O tipo de Atores definidos à priori pela Associação DNS.PT são:

- Responsável pela Qualidade ou Segurança da Informação (CISO/RS): Despoleta o processo de gestão de risco, e efetua a verificação dos relatórios enviados;

- Dono do Ativo ou Processo: Lista os seus Ativos ou Processos, faz o levantamento dos riscos associados a eles e procede à elaboração do relatório da análise de risco;

- Responsável pelo Risco: Com base no relatório de análise de risco, elabora um plano de tratamento de risco. Atualmente esta função é desempenhada pelo CISO/RS;

- Responsável pelo Controlo: Após a aceitação do plano de tratamento de risco por parte do Conselho Diretivo, implementa os controlos definidos. Atualmente esta função é desempenhada pelo CISO/RS;

- Conselho Diretivo: Toma a decisão final sobre aceitação ou recusa do plano de tratamento de risco.

Para facilitar a compreensão, os Casos de Uso foram divididos em quatro grupos, com base na descrição fornecida pela Associação DNS.PT.

Análisar o Risco

Atualmente a análise do risco é realizada de forma diferente dependendo se a entidade sobre a qual os Riscos estão a ser analisados é um Ativo ou um Processo. A diferença reside na dimensão da avaliação do impacto, sendo que atualmente os Ativos são avaliados mediante a Qualidade e os Processos segundo a Segurança de Informação.

Na Figura 3.10 e 3.11 encontram-se representados respetivamente os casos de uso para a análise de risco relativa a Ativos e Processos. As funções do CISO/RS incluem toda a gestão dos ativos e dos processos: listagem, criação e descontinuação dos mesmos, e a aglomeração das análises realizadas. Os Donos dos Ativos ou dos Processos por sua vez estão encarregues de análisar os Ativos ou Processos, identificar os riscos a eles inerentes e elaborar um relatório de análise de risco para os ativos a ele associado e devolver este relatório ao CISO/RS.

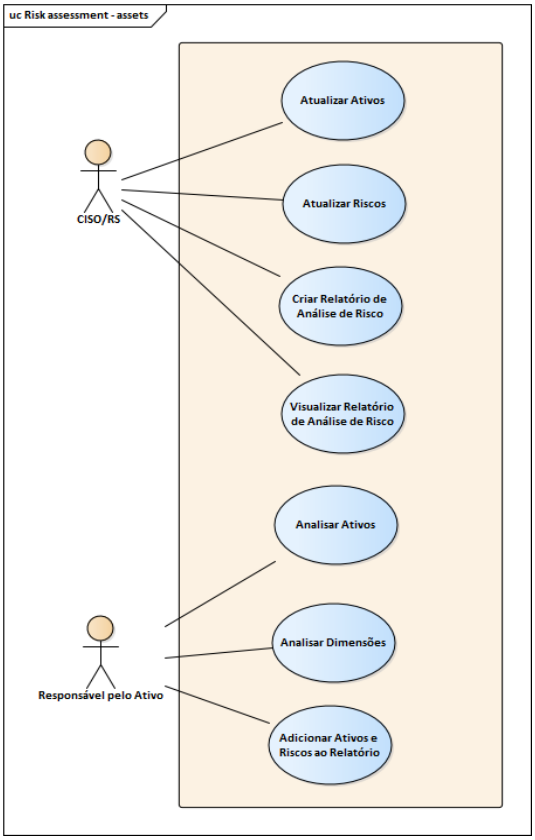

Figura 3.10: Diagrama de Caso de Uso - Análise de Riscos (Ativos).

Criação do Plano de Tratamento de Risco

Após a análise do risco, o próximo passo consiste em fazer uma apreciação e avaliação dos riscos calculados. Atualmente o responsável pela apreciação e avaliação dos Riscos é o CISO/RS sendo ele igualmente o responsável pela listagem, criação e descontinuação dos Riscos.

Nesta fase são sinalizados os riscos cujo valor calculado na fase anterior supere o limite definido, pela Associação DNS.PT. Qualquer impacto cujo valor se enquadre no escalão de “Muito Grave” deverá pro-

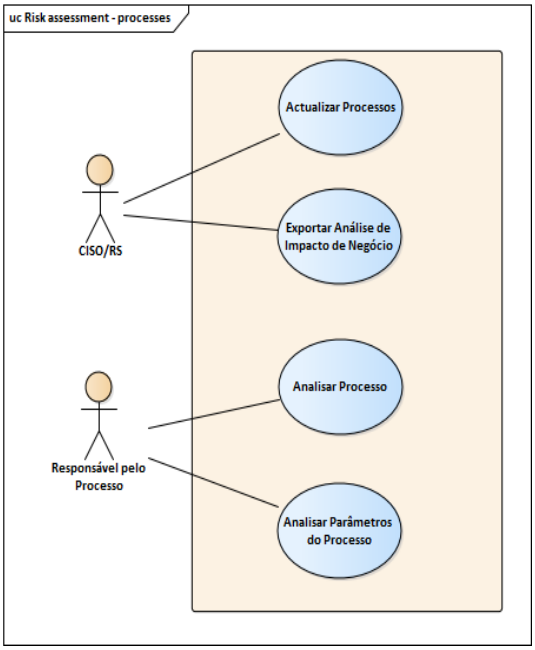

Figura 3.11: Diagrama de Caso de Uso - Análise de Riscos (Processos).

ceder para a fase de tratamento. É produzida uma tabela onde é possível visualizar todos riscos que necessitam que lhe sejam aplicadas medidas (Controlos) para que se reduza o nível de risco para valores aceitáveis. Todos os Controlos que irão ser implementados são registados no ”Plano de Tratamento de Risco”. O Caso de Uso que engloba estas atividades pode ser visto na Figura 3.12.

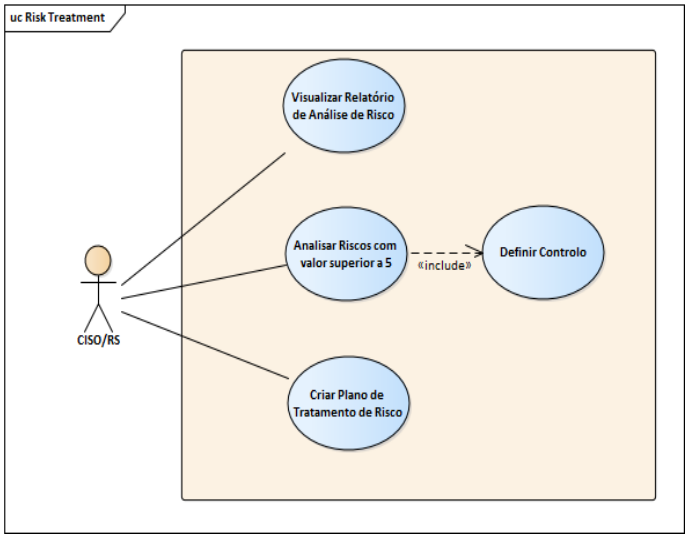

Figura 3.12: Diagrama Caso de Uso - Criação do Plano de Tratamento de Risco.

Aplicação de Controlos

Os Controlos são geridos igualmente pelo CISO/RS, que deverá tomar as medidas necessárias junto dos Donos dos Ativos ou Processos para estes sejam cumpridos. Para que o Plano de Tratamento de Risco seja aprovado existe um conjunto mínimo de informação que deverá constar:

- Controlo a implementar;
- Risco associado;
- Responsável pela Implementação;
- Custo estimado;
- Início e fim do projeto estimado.

Os termos da aplicabilidade das normas ISO 22301:2012 e ISO 27001:2015 também poderão ser exportados da aplicação informática sob a forma de uma declaração de aplicabilidade e entregues ao Conselho Diretivo. O Caso de Uso referente a estas atividades pode ser observado na Figura 3.13.

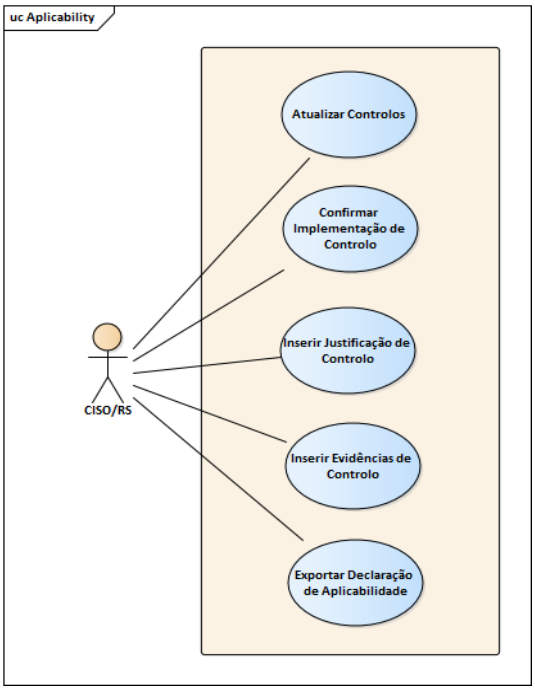

Figura 3.13: Diagrama Caso de Uso - Aplicação de Controlos.

Definição de Responsabilidades

A atribuição de responsabilidade é feita através de uma tabela de RACI (Matriz de Atribuição de Responsabilidades). Esta tabela de RACI descreve a participação dos vários utilizadores na conclusão das tarefas. Atualmente quem gere esta tabela é o CISO/RS, podendo acrescentar novos papéis e posteriormente atribui-los aos utilizadores respetivos. Na Figura 3.14 encontra-se o Caso de Uso respetivo.

3.2.3 Aplicação Informática - Utilização

Nesta secção irá ser descrita a lógica de funcionamento da aplicação informática do ponto de vista do utilizador, tal como as principais dificuldades identificadas. A aplicação encontra-se atualmente instalada no computador de trabalho do CISO/RS, sendo apenas daquela máquina que é possível aceder ao sistema.

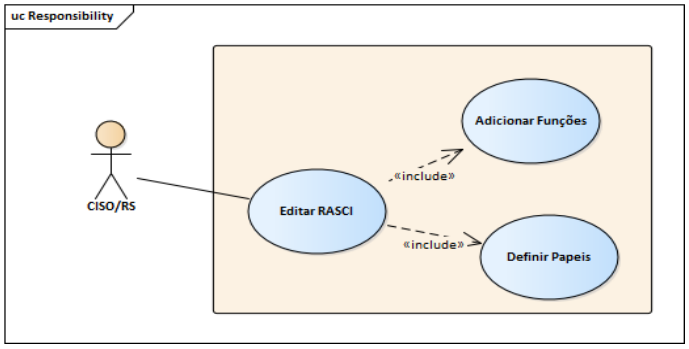

Figura 3.14: Diagrama Caso de Uso - Definição de Responsabilidades.

É necessário o CISO/RS deslocar-se fisicamente aos restantes colaboradores para que estes possam completar as suas funções no decorrer do processo de gestão de risco. Foi esta dificuldade que despoletou o requisito inicial da Associação DNS.PT de que a nova versão da aplicação estivesse disponível remotamente para que pudesse ser acedida através da rede interna (Sistema Ative Directory). A aplicação dispõe de cinco menus principais, acessiveis através de uma barra horizontal no topo do ecrã (Figura 3.15):

- **Framework:** Usado para criar, configurar e gerir o conjunto de artefactos da aplicação;
- **Assessment:** Permite gerir e criar as análises de risco e planos de tratamento;
- **Reports:** Tem como objetivo a extração de documentos, relatórios e listas de entidades.
  - Lista de Ativos;
  - Lista de Riscos;
  - Lista de Processos;
  - Lista de Dependência de Ativos;
  - Lista de Estado de Indicadores Monitorização;
  - Análise de Risco;
  - Plano de Tratamento do Risco;
  - Análise de Impacto de Negócio;
  - Declaração de Aplicabilidade;
  - Lista das Partes Interessadas.
- **Config:** Configuração de parâmetros da aplicação como:
  - Tipos de ativos;
  - Escala de Impacto (Figura 3.16) e Probabilidades;
  - Responsáveis;
  - Classificação de Informação.

Figura 3.15: Interface da Aplicação.

Figura 3.16: Matriz de Impacto do Risco.

3.3 Definição do Problema

Nesta secção irão ser formalmente definidos os problemas que se pretendem resolver, a solução elaborada e os objetivos que se pretende atingir.

Os principais necessidades identificadas pela Associação DNS.PT no início do projeto foram a necessidade de simplificar a lógica da aplicação, tornando-a mais intuitiva ao uso, e quebrar a restrição fisíca de apenas estar instalada numa máquina o que faz com que seja necessário ao gestor do sistema deslocar-se para realizar as atividades com os restantes utilizadores. Da análise realizada, e apresentada na secção anterior, chegou-se às seguintes conclusões:

- Apesar do modelo de dados utilizado pela aplicação suportar o processo de gestão de risco, a sua estrutura e organização faz com que seja complicado identificar as principais entidades envolvidas no processo, melhorar o modelo e captar erros e não conformidades;
- A representação da camada de aplicação desenvolvida afere uma necessidade de especificar os componentes da mesma para além dos ”Sistemas de Informação”, referidos na documentação da

organização;

- Os requisitos levantados junto da Associação DNS.PT identificam um conjunto mais alargado de casos de usos que ainda não foram definidos;

- A necessidade de separar definitivamente as funções dos responsáveis pelos vários objetos da aplicação. Das reuniões com a organização foram delimiados um outro conjunto de tipos de utilizadores, o que aumenta ainda mais o grau de complexidade da aplicação.

Tal como foi referido no Capítulo 1, foi realizada uma análise inicial à complexidade dos requisitos apresentados pela Associação DNS.PT e às necessidades que iam sendo identificadas. Chegou-se à conclusão que uma reformulação total do suporte digital estaria para além do âmbito que seria possível realizar deste projecto.

O projeto foi então orientado para que os resultados obtidos pudessem acrescentar suficiente valor à organização. Os objetivos do projeto foram redefinidos como:

- Elaborar representações dos vários processos, aplicações e tecnológias da Associação DNS.PT e das dependências entre eles. O objetivo final: Ter disponível para a organização uma documentação estensa sobre os seus diveros componentes;

- Fazer um levantamento de todos os componentes da aplicação informática, desde o modelo de dados utilizado até aos seus Casos de Uso;

- Com base nos dois pontos referidos anteriormente, produzir um documento de requisitos para a organização, para auxiliar futuras implementações e onde estivessem contemplados possíveis pontos de melhoria.

Os dois primeiros pontos já tinham sido iniciados quando se começou a analisar a organização e a aplicação de gestão de risco. O trabalho a ser realizado passou por dar seguimento ao estudo realizado e alinhar os conteúdos produzidos com os objetivos da organização.

Capítulo 4

Proposta de Solução

Neste capitulo irá ser apresentadas e descritas as propostas de melhoria elaboradas para dar resposta às necessidades da Associação DNS.PT. Estas tiveram em conta as necessidades operacionais da organização e os interesses dos seus *stakeholders*.

4.1 Simplificação do Modelo de Dados

Começou-se por desenvolver de raiz o modelo de dados utilizado, identificando os conceitos e entidades essenciais para suportar o processo de gestao de risco. Foram sugeridas as seguintes mudanças ao modelo de dados:

- Definição e simplficação das entidades sobre quais o risco vai ser analisadas através da aglomeração das entidades ”Processo”, ”Sistema de Informação”e ”Informação”, sob a entidade ”Ativo”simplificando assim a estrutura do modelo;
- Identificação para cada tipo de ”Ativo”, de quais os indicadores de desempenho que serão analisados, definindo a entidade ”Indicador”como uma entidade separada e que caracteriza cada tipo de ”Ativo”. Os Indicadores são um conjunto de métricas definidas, orientadas à estratégia organizacional, que têm como objetivo definir as metas a alcançar.
- Associação de um ”Responsável”a cada ”Ativo”, ”Risco”, ”Controlo”e ”Indicador”, uma vez que cada utilizador puderá ficar associado a uma ou mais dessas entidades
- Definição das entidades ”Análise de Risco”e ”Plano de Tratamento de Risco”como o resultado da relação ”Ativo-”Risco”e ”Risco-”Controlo”respetivamente;
- Definição da relação da ”Parte Interessada”com as restantes entidades, de forma a assegurar a comunicação com os *stakeholders* ao longo do processo.

O modelo de dados redesenhado retrata as principais entidades do processo de gestão de risco e as relações entre elas 4.1.

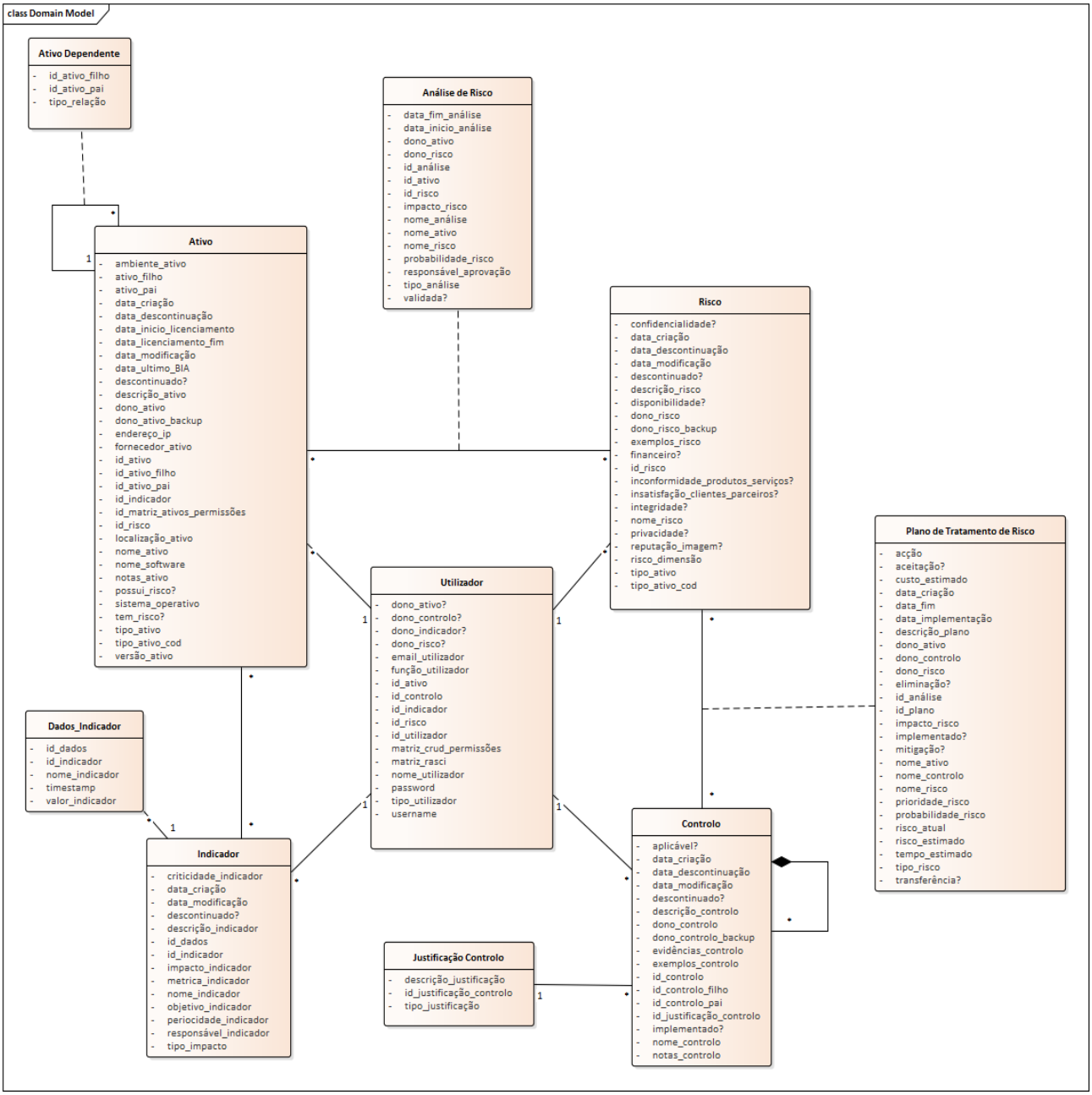

Figura 4.1: Diagrama UML - Proposta do Modelo de Dados para a Aplicação Informática.

Adicionalmente, e uma vez que uma das necessidades identificadas durante a análise foi a maior definição dos papéis dos utilizadores da aplicação, criou-se um Diagrama UML com o objetivo de explorar o conceito de Utilizador e complementar o diagrama referido anteriormente (Figura 4.2). Para garantir que não existe perda de informação caso a Associação DNS.PT decida implementar esta arquitetura, é apresentada na Tabela C.1, Anexo C, um modelo de migração de atributos de um modelo para

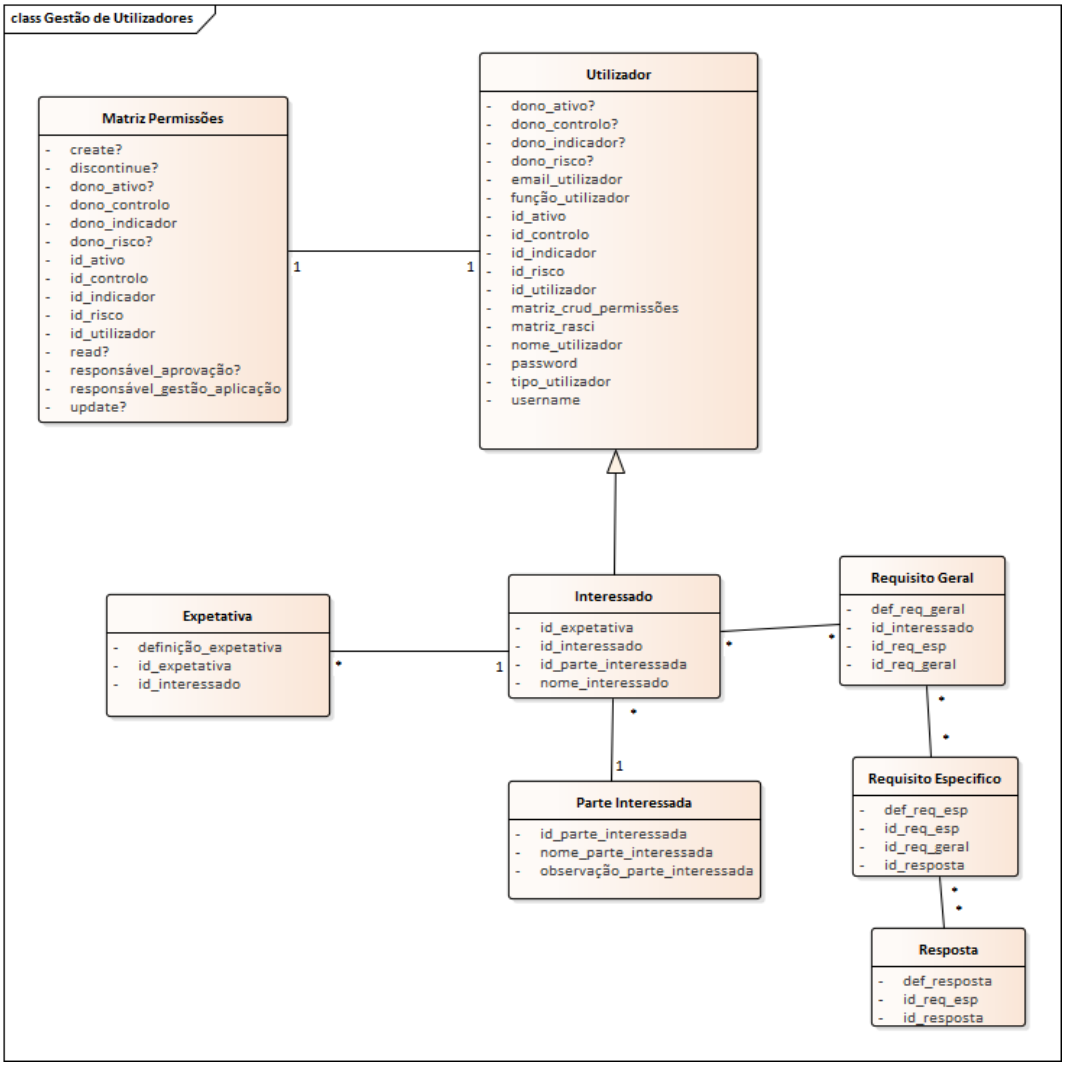

Figura 4.2: Diagrama UML - Modelo de Dados para a Gestão de Utilizadores.

4.2 Reestruturação dos Componentes envolvidos no Processo de Negócio FP.02

Após analisar as várias representações da Associação DNS.PT criadas em Archimate, foi desenvolvida uma arquitetura alternativa para os diversos diagramas criados tendo como base as regras definidas pela nomenclatura Archimate. Na Figura 4.3, encontra-se um exemplo de uma destas representações desenvolvidas, como alternativa à vista geral de todos os componentes relacionados com o Processo de Negócio FP.02. As diferenças entre esta representação e a da Figura 3.8, do Capitulo 3 são:

- Adoção completa da nomenclatura Archimate: Alterar a designação de ”Sistemas de Informação”para ”Serviços Aplicacionais”;
- Acrescentar componentes Archimate ausentes, como a lista de componentes ”Interfaces Aplicacionais”através dos quais os Processo de Negócio acedem aos Serviços Aplicacionais, aumentado o nível de detalhe na representação da organização;
- Especificação da Funcionalidade da Aplicação Informática ”Serviço de Gestão de Dados”.

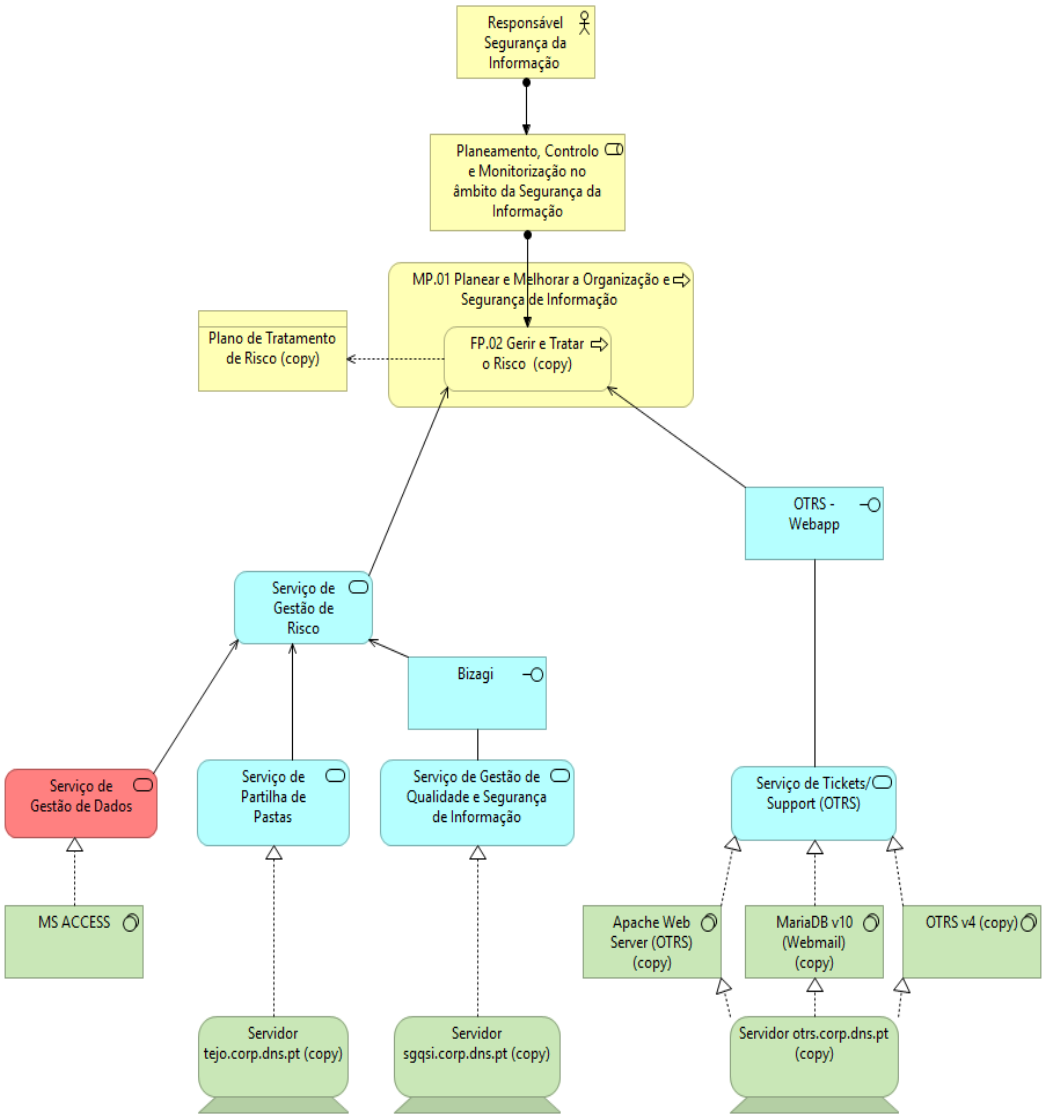

Figura 4.3: Componentes do Processo de Gestão de Risco da Associação DNS.PT.

Um dos pontos principais que a análise identificou foi que a Camada de Aplicação se encontrava pouco detalhada, não havendo documentação suficiente para ir a um nível de granularidade mais elevado relativamente às entidades dessa camada. Esta abordagem permite também definir mais claramente a funcionalidade prestada pela aplicação informática que se encontra-se sinalizada a vermelho, enquanto aplicação que suporta o processo de gestão de risco enquanto ferramenta de gestão documental.

4.3 Reformulação dos Casos de Uso

Esta proposta passa pela reavaliação das funcionalidades da aplicação e a definição dos novos tipos de utilizadores. Os novos tipos de utilizadores deverão estar diretamente ligados às ações e aos cargos que estes têm durante o processo de gestão de risco. Estes perfis não são mutuamente exclusivos, ou seja, o Responsável pela Aprovação pode ser igualmente Dono de um Ativo, por exemplo. Os perfis de utilizadores propostos são:

- Responsável pela Gestão da Aplicação;

- Responsável pela Aprovação;
- Donos de Ativos, Riscos, Controlos e Indicadores;
- Colaborador: Qualquer um dos tipos referidos anteriormente.

Caso de Uso - Gestão de Ativos

Os Ativos são recursos que sustentam a informação e negócio da Associação DNS.PT. A Gestão de Ativos permitirá aos Donos dos Ativos não só gerirem o ciclo de vida dos seus Ativos (Criação, Modificação e Descontinuação), mas também desempenharem as suas funções aquando realização da análise do risco. Na Figura 4.4 encontra-se representado o diagrama do Caso de Uso relativo a esta funcionalidade.

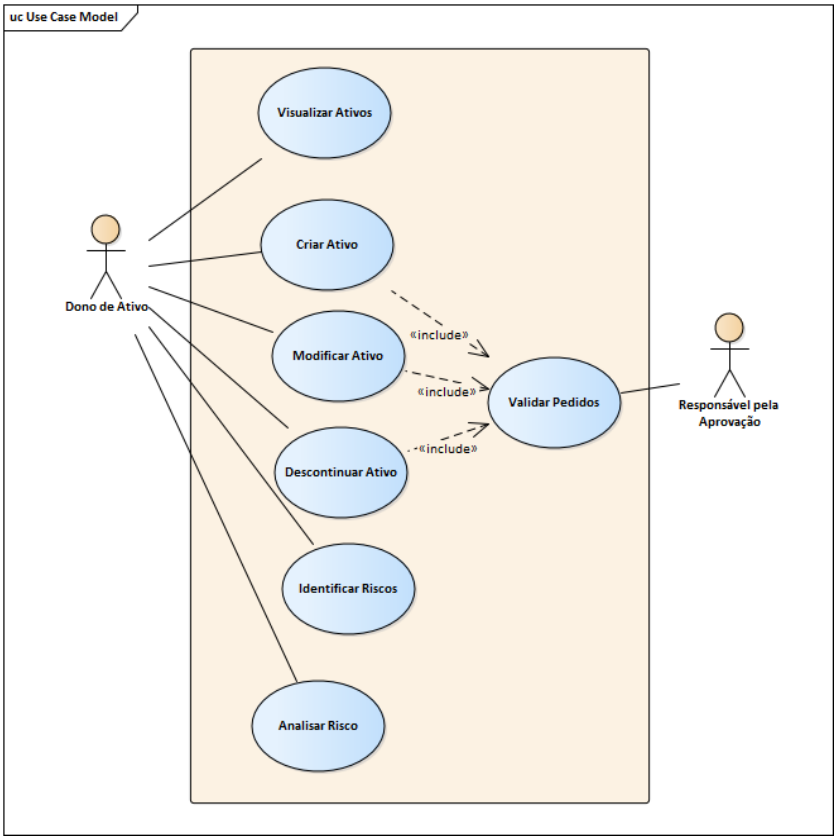

Figura 4.4: Diagrama Caso de Uso - Gestão de Ativos

Esta funcionalidade permitirá:

- Visualizar todos os Ativos que o Utilizador tenha permissões para ver e os quais ele é Dono;
- Criar, alterar ou descontinuar um Ativo, caso o utilizador tenha permissões para tal, estando sempre sujeito à aprovação pelo Responsável pela Aprovação;
- Caso os Ativos do qual o Utilizador é Dono tenham uma análise de risco pendente, serão destacados e o Dono será notificado;
- O Dono do Ativo poderá realizar a análise do Risco sobre os Ativos destacados e selecionados, o que inclui:

- Identificar os Riscos relativos aos Ativos em questão;
- Analisar o Risco: quantificando o impacto e a probabilidade do Risco no Ativo mediante os Indicadores a eles associados.

Caso de Uso - Gestão de Riscos

A Gestão de Risco permitirá aos Donos do Riscos gerirem os Riscos a que eles estão associados e desempenharem as suas funções durante a fase de avaliação de riscos e criação do Plano de Tratamento de Risco. Este Caso de Uso encontra-se representado na Figura 4.5.

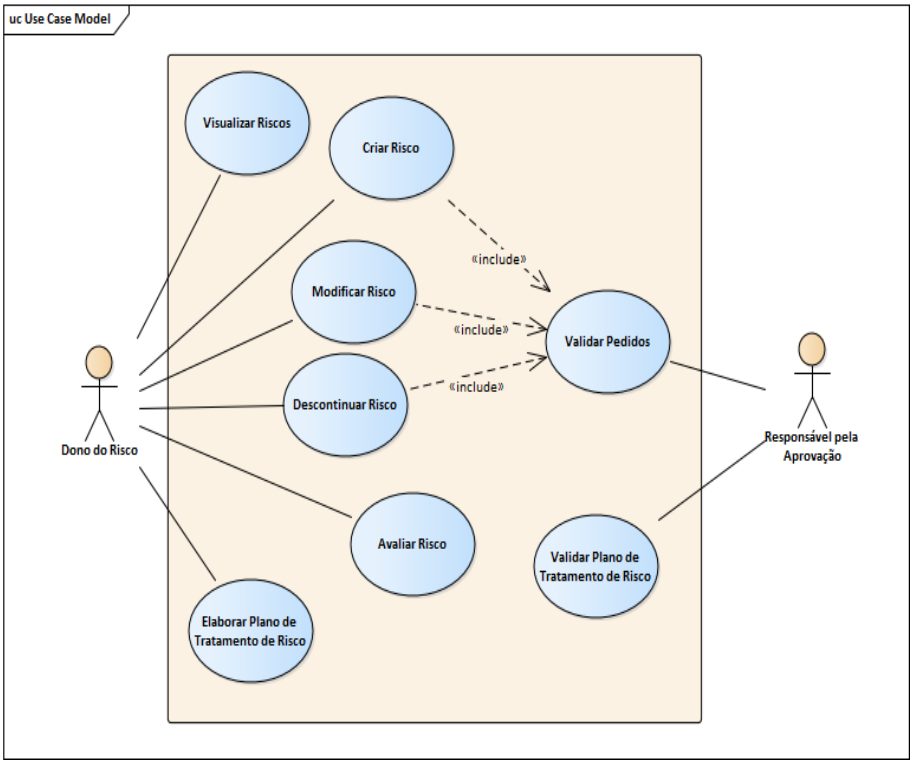

Figura 4.5: Diagrama Caso de Uso - Gestão de Riscos

Esta funcionalidade permitirá:

- Criar, alterar ou descontinuar um Risco, caso o utilizador tenha permissões para tal, estando sempre sujeito a aprovação pelo Responsável pela Aprovação;
- Visualizar todos os Riscos que o Utilizador tenha permissões para ver e os quais ele é Dono;
- Caso exista uma avaliação de riscos pendente, os riscos associados a essa avaliação serão realçados e o Dono será notificado.

Caso de Uso - Gestão de Controlos

A Gestão de Controlos permitirá gerir o ciclo de vida dos Controlos e finalizar o processo de tratamento de risco. A representação para este Caso de Uso encontra-se na Figura 4.6.

Esta funcionalidade permitirá:

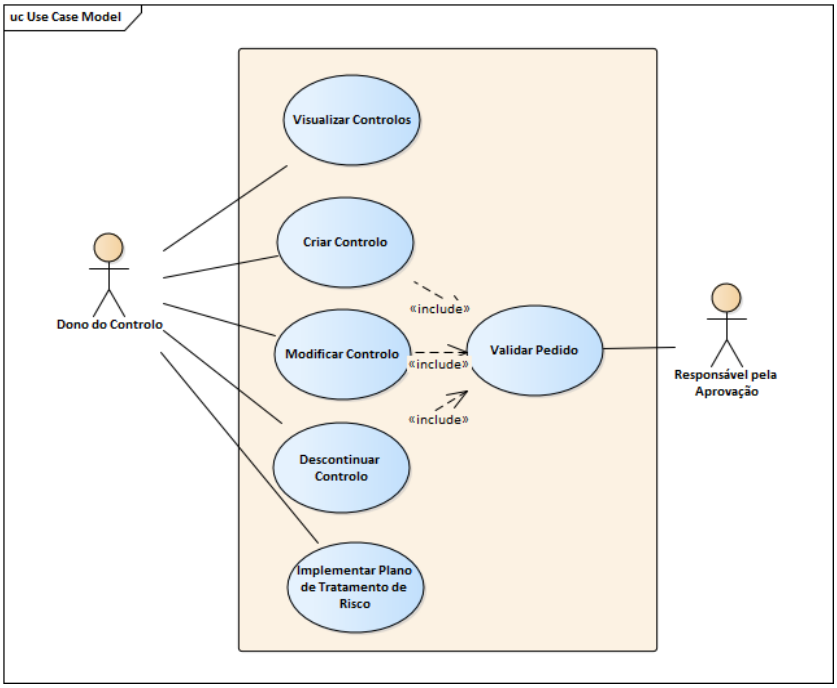

Figura 4.6: Diagrama Caso de Uso - Gestão de Controlos

- Criar, alterar ou descontinuar um Controlo, caso o utilizador tenha permissões para tal, estando sempre sujeito a aprovação pelo Responsável pela Aprovação;
- Visualizar todos os Controlos que o Utilizador tenha permissões para ver e os quais ele é Dono;
- Caso haja um Plano de Tratamento aprovado pelo Conselho Diretivo, os Controlos associados a esse Plano serão destacados para que o Dono os possa concretizar. Será igualmente notificado pelo Serviço de Notificações.

Casos de Uso - Gestão de Indicadores

A Gestão de Indicadores irá permitir aos Colaboradores acederem diretamente aos valores dessas métricas associados aos Ativo da organização. O diagrama de Caso de Uso encontra-se representado na Figura 4.7.

Esta funcionalidade permitirá:

- Criar, alterar ou descontinuar Indicadores, sendo que esta revisão dos Indicadores é feita periodicamente pelo Responsável pela Gestão do Sistema;
- A visualização dos Indicadores e dos seus Dados por qualquer Colaborador da associação DNS.PT;
- Importação ou Exportação dos dados das métricas relativo a um ou mais Indicadores, por parte do Dono do Indicador.

Caso de Uso - Revisão Documental

A aplicação informática permitirá igualmente à Associação DNS.PT rever e analisar toda a documentação pertinente não só a nível do processo de gestão de risco, mas também a nível do negócio (Figura 4.8).

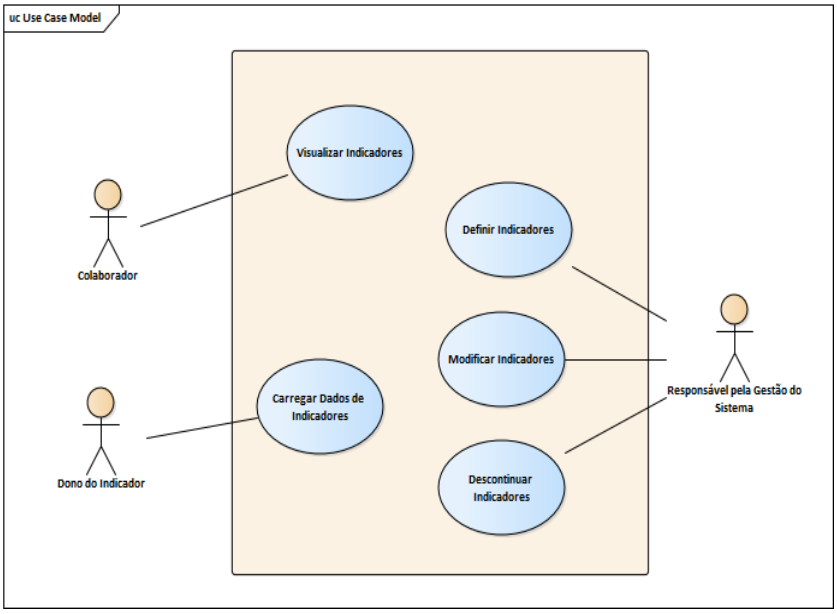

Figura 4.7: Diagrama Caso de Uso - Gestão de Indicadores

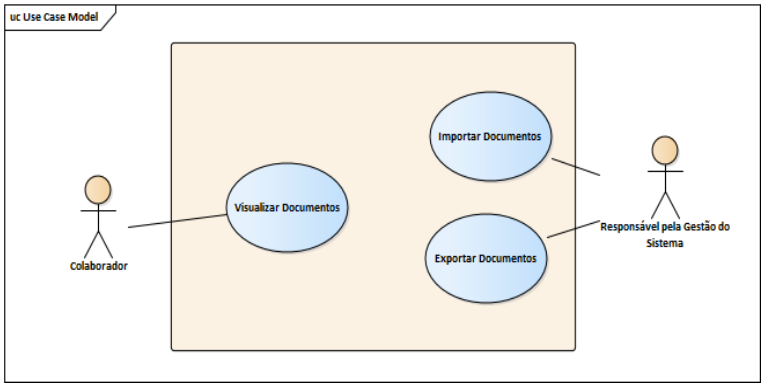

Figura 4.8: Diagrama Caso de Uso - Revisão Documental.

Esta funcionalidade permitirá:

- A visualização de documentos tais como, legislações, normas e declarações de aplicabilidade;
- Importação e Exportação de documentos por parte do Responsável pela Gestão do Sistema.

Caso de Uso - Autenticação

Um dos principais requisitos levantados pela Associação DNS.PT foi a criação de diferentes tipos de perfis de utilizadores para diferentes tipos de acessos e permissões sobre a aplicação. Propõe-se que o mecanismo de autenticação seja integrado com a atual integrado Serviço de Active Directory da DNS.PT. Estes requisitos foram modelados no caso de uso da Figura 4.9

Caso de Uso - Notificação

O objetivo desta funcionalidade é permitir a comunicação entre utilizadores, seja através de um serviço

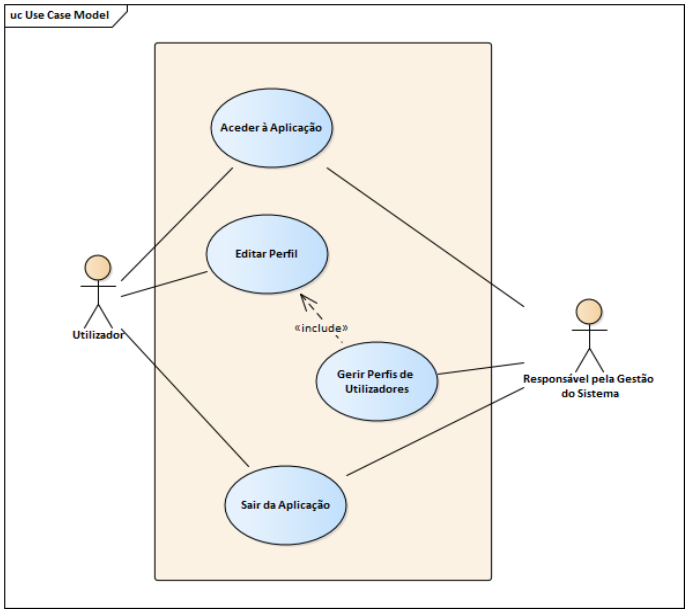

Figura 4.9: Diagrama Caso de Uso - Autenticação

implementado na aplicação, ou através do envio e receção de mensagens usando serviços externos (pex: email).

Esta funcionalidade deverá facilitar não só a comunicação individual entre Utilizadores, mas também agilizar o processo de gestão de risco através da capacidade de enviar documentos e notificações. Esta funcionalidade está representada no diagrama de Caso de Uso da Figura 4.10.

Caso de Uso - Carregamento e Descarregamento de Ficheiros

A aplicação informática deverá permitir o carregamento e descarregamento de ficheiros com formatos standard (pex: office, csv, json, xml, etc...). Este caso de uso encontra-se modelado na Figura 4.11.

Caso de Uso - Configurabilidade

A aplicação deverá permitir ao Responsável pela Gestão da Aplicação definir os acessos à aplicação, as variáveis globais (pex: tempos de envio de pedidos acumulados), e permissões CRUD sobre os Ativos, Riscos, Controlos e Indicadores. Na Figura 4.12 encontra-se representada esta funcionalidade.

Caso de Uso - Rastreamento de Acções

Armazenamento de informação sobre o conjunto das ações que foram realizadas na aplicação e quem as realizou (ex: Logs com timestamp) e manter em registo a lista de Objetos (ex: Ativos, Riscos, Controlos, Indicadores) descontinuados. (Figura 4.13)

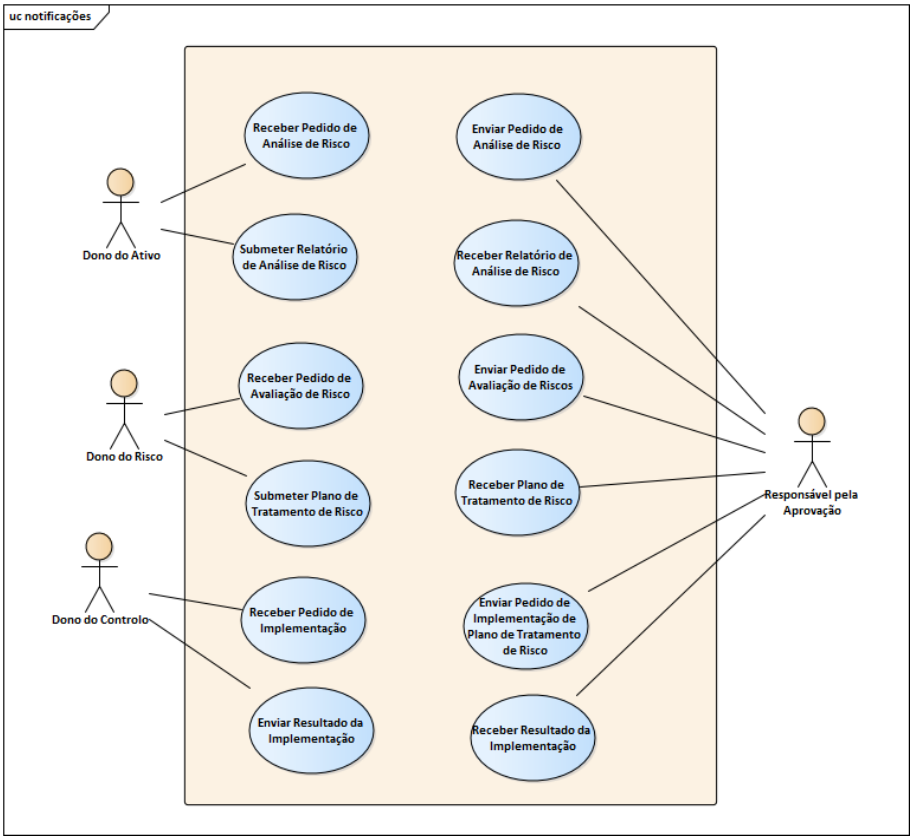

Figura 4.10: Diagrama Caso de Uso - Notificação.

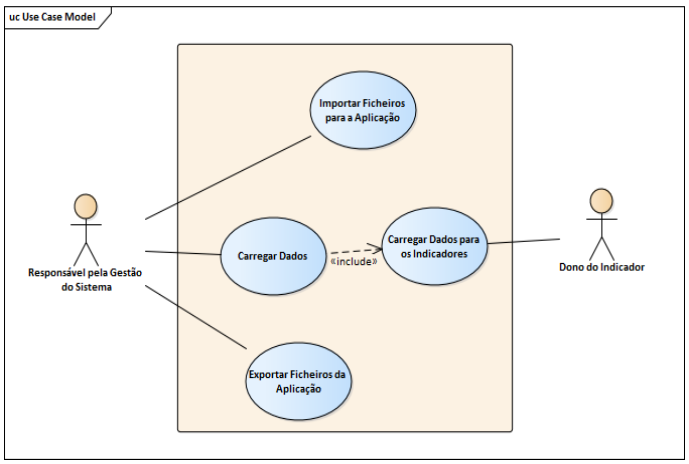

Figura 4.11: Diagrama Caso de Uso - Carregamento e Descarregamento de Ficheiros.

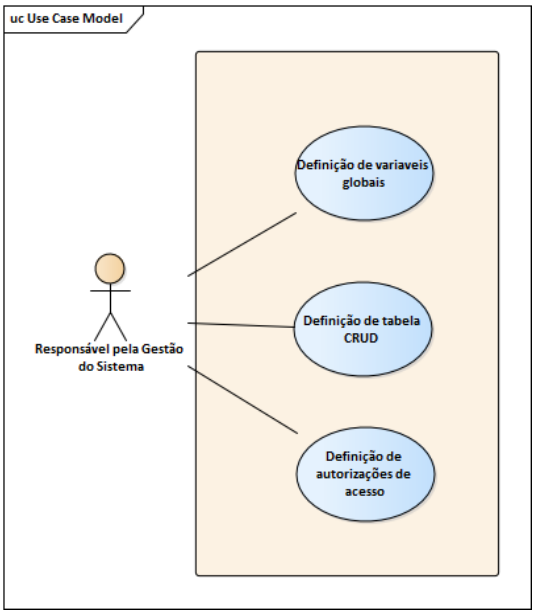

Figura 4.12: Diagrama Caso de Uso - Configurabilidade.

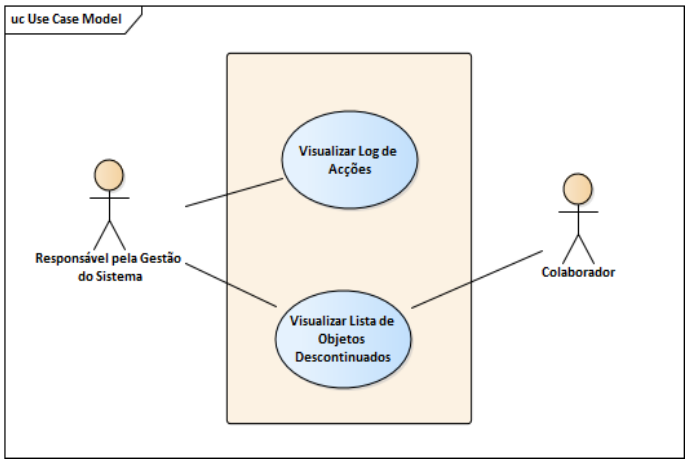

Figura 4.13: Diagrama Caso de Uso - Rastreabilidade.

Capítulo 5

Conclusão e Trabalho Futuro

Durante este trabalho foi possível aprofundar os meus conhecimentos relativos às normas ISO, mais concrentamente a norma ISO 22301:2012 e a norma ISO 31000:2009. A realização do estágio na Associação DNS.PT permitiu-me também ter um acesso privilegiado a informações, tais como a estrutura e processos implementados na organização. Foi igualmente importante ter pudido assistir ao funcionamento aplicação, em primeira pessoa, e puder estudar como os colaboradores da organização a utilizavam assim como quais as principais necessidades existentes. Isto apenas foi possível com a ajuda e apoio da Associação DNS.PT.

O objetivo inicial do trabalho era efetivamente desenvolver uma nova versão da aplicação informática, no entanto como já foi descrito, este âmbito acabou por ser ajustado face à realidade do esforço que seria necessário para alcançar os objetivos esperados. O principal valor que este trabalho adicionou à organização foi permitir que esta tivesse um maior suporte documental na qual basear futuros desenvolvimentos da aplicação. A documentação desenvolvida incluiu:

- Listagem de todos os Processo de Negócio, Aplicações, Sistemas e Tecnologias utilizadas;
- Representação das relações entre os diversos componentes da organização, utilizando a linguagem Archimate, em três camadas diferentes:
  - Camada de Negócio;
  - Camada de Aplicação;
  - Camada de Tecnologia;
- Levantamento de melhorias principalmente a nível dos Componentes de Aplicação;
- Representação do Modelo de Dados atual da aplicação informática utilizando EA;
- Modelação dos Casos de Uso atuais da aplicação informática;
- Elaboração de um Modelo de Dados alternativo que suporte as necessidades e requisitos da organização;
- Definição de Tabelas de Migração entre os Modelos de Dados;
- Definição dos Casos de Uso necessários para suportar os requisitos da organização e que utilizem o modelo de dados redesenhado.

Apesar do valor acrescido deste trabalho não conter uma apresentação de tecnologias alternativas para suportar a aplicação, estabelece vistas que tornarão mais fácil a escolha destas tecnologias.

A revisão, análise, representação e criação de documentação realizada são uma boa base de trabalho para numa seguinte fase se proceder à implementação Desta forma, os objetivos propostos para este trabalho foram atingidos culminando na elaboração do relatório de análise entregue à Associação DNS.PT.

A literatura descreve frequentemente o risco como a possibilidade de sofrer danos ou perdas. Apesar desta definição, aparentemente tão negativa e pessimista, somos todos confrotados com risco no nosso dia-a-dia, e esses riscos podem ter consequências que se manifestam no seguinte momento como dai a alguns anos. A incerteza faz com que o uso deste tipo de ferramentas seja cada vez mais útil e recompensador. Espero que com este projeto tenha sido capaz de contibuir para dar à Associação DNS.PT um futuro menos incerto e mais seguro.

Bibliografia

[1] Risk and Insurance Management Society Inc., “RIMS Risk Maturity Model (RMM) for Enterprise Risk Management.”

[2] International Organization for Standardization, “ISO 22300:2012 Societal Security — Terminology,” 2012.

[3] International Organization for Standardization, “ISO 22301:2012 Societal Security — Business continuity management systems — Requirements,” 2012.

[4] International Organization for Standardization, “ISO Guide 73:2009: Risk Management Vocabulary,” 2009.

[5] International Organization for Standardization, “ISO / FDIS 31000 Risk Management - Principles and Guidelines,” 2009.

[6] Prof. Dr. Olaf Passenheim, *Enterprise Risk Management*. 2013.

[7] Casual Actuarial Society Enterprise Risk Management Committee, “Overview of Enterprise Risk Management,” May 2003.

[8] Committee of Sponsoring Organizations of the Treadway Commission, “Enterprise Risk Management — Integrated Framework: Executive Summary,” 2004.

[9] João Carlos Gonçalves Fialho, “Risk management process for security of the information and business continuity,” Master’s thesis, Instituto Superior Técnico, 2016.

Apêndice A

Modelo de Dados

A.1 Modelo de Dados AS-IS extraído do Microsoft Access

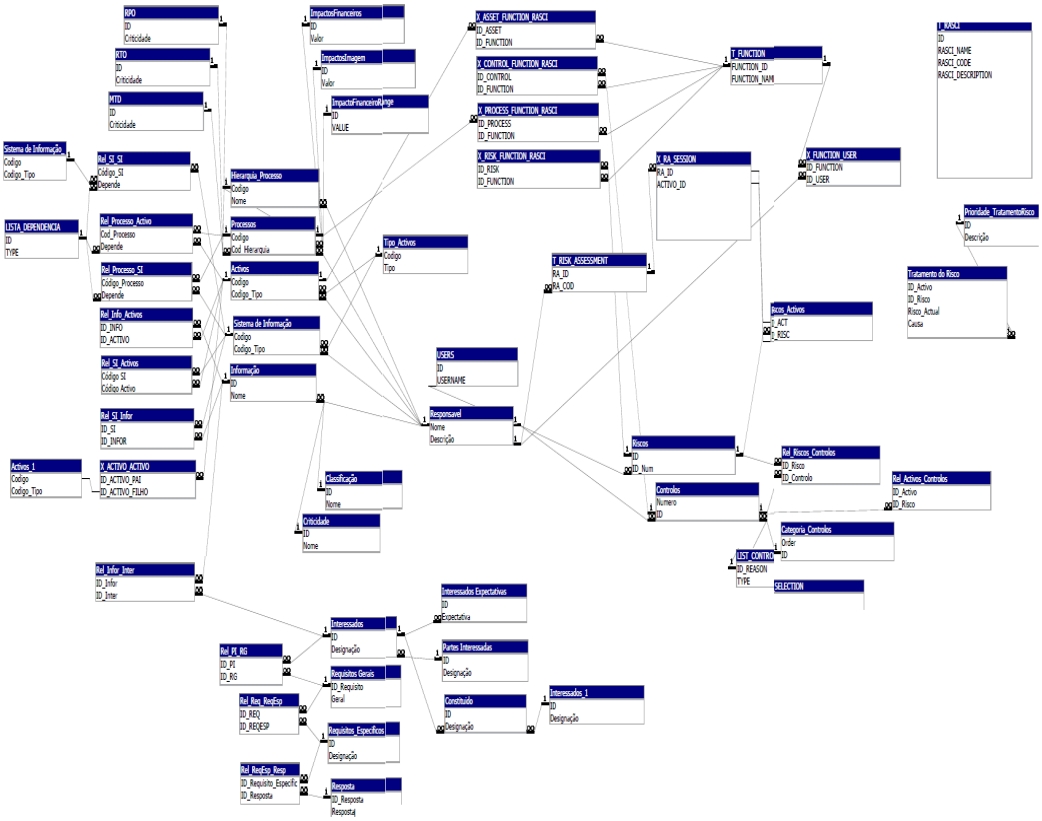

Figura A.1: Modelo de Dados da Aplicação Informática extraido do Microsoft Access.

Apêndice B

Listagem das Entidades da Associação DNS.PT

B.1 Camada de Negócio

MacroProcessos	**Processos**
MP.01 Planear e Melhorar a Organização e Segurança de Informação	FP.01 Planear e Rever FP.02 Gerir e Tratar o Risco FP.03 Controlar e Monitorar a Atividade FP.04 Gerir Ocorrências.
MP.02 Comunicação e Imagem	FP.05 Comunicação e Imagem
MP.03 Gestão da Responsabilidade Social Corporativa	FP.06 Realizar Iniciativa FP.07 Acreditação de Sites: Confio.pt
MP.04 Gestão de Pessoas	FP.08 Recrutar, Selecionar e Integrar Pessoa FP.09 Gerir Funções e Carreiras FP.10 Gerir Formação FP.11 Avaliar Desempenho FP.12 Gerir Saída de Pessoa FP.13 Gestão Quotidiana da Pessoa
MP.05 Gestão de Projetos	FP.14 Gestão de Projetos
MP.06 Gestão de Recursos Financeiros	FP.15 Gestão de Compras FP.16 Gerir Contratos FP.17 Avaliar Fornecedores FP.18 Efetuar Inventário FP.19 Gestão Financeira Quotidiana
MP.07 Registo e Gestão de Nomes de Domínio .PT	FP.20 Registar Domínios FP.21 Gerir Relação com Clientes FP.22 Monitorizar Domínios FP.23 Gerir Problemas Jurídicos FP.24 Gerir Pagamentos FP.25 Alterar e Transferir Domínios FP.26 Remover Domínios FP.27 Propagação da Zona .PT

Tabela B.1: Processos de Negócio da Associação DNS.PT

B.2 Camada de Aplicação - Lista de Componentes de Aplicação

- Sistema Website DNS.PT;
- Sistema de Gestão de Risco;
- Sistema de Gestão da Qualidade e Segurança de Informação;
- Sistema de Assiduidade;
- Sistema Backup;
- Sistema Email;
- Sistema de Partilha de Pastas;
- Sistema Financeiro X3 - Gestão Financeira;
- Sistema EPP - Registo de Domínios por Registrars;
- Sistema de DNS Interno;
- Sistema SIGA - Registo de Domínios por Registrants;
- Sistema DNSSEC - Segurança dos Domínios;
- Sistema de Delegação de Domínios .PT;
- Sistema ERP Primavera;
- Sistema de Digitalização e Impressão;
- Sistema Saperion - Gestão Documental;
- Sistema de Monitorização;
- Sistema de Active Directory - Autenticação Interna;
- Sistema de Antivirus;
- Sistema de Gestão;
- Sistema Whois;
- Sistema OTRS - Tickets/Suporte.

B.3 Camada Tecnológica - Lista de Sistemas de Software

- BIND
- Apache Tomcat (Saperion)
- Microsoft SQL Server 2012
- Saperion v7.5
- SQLBackupAndFTP v10
- Anubis Mail Protection System
- Dovecot
- Postfix
- RoundCube Mail
- Apache Web Server (WEBMAIL)
- MariaDB v10 (Webmail)
- Software Primavera ERP
- Microsoft SQL Server 2012 (ERP)
- EPP Server
- Gestor de Conteudos (CMS) da Seara
- Apache Web Server (OTRS)
- OTRS v4
- MariaDB v10 (otrs)
- Software BIND DNSSEC
- ZABBIX
- DNS Statistics Collector
- MS Office
- Millenium 3
- Whois Server
- Software Base de Dados – Oracle
- Software X3
- Software Bacula (Backups)

Apêndice C

Tabela de Migração de Atributos

Modelo Atual	Modelo Proposto
PROCESSO.BACKUP_OWNER_NAME	ATIVO.dono_ativo_backup
PROCESSO.BIA_date	ATIVO.data _ultimo _BIA
PROCESSO.COD _Hierarquia	ATIVO.id _ativo _pai
PROCESSO.COD_ImpactoFinanceiro	ATIVO.id_indicador
PROCESSO.COD_ImpactoFinanceiroRange	ATIVO.id_indicador
PROCESSO.COD_ImpactoImagem	ATIVO.id_indicador
PROCESSO.COD_MTD	ATIVO.id_indicador
PROCESSO.COD_RPO	ATIVO.id_indicador
PROCESSO.COD_RTO	ATIVO.id_indicador
PROCESSO.Codigo	ATIVO.id_ativo
PROCESSO.data_descontinuado	ATIVO.data_descontinuação
PROCESSO.Descontinuado	ATIVO.descontinuado?
PROCESSO.Descrição	ATIVO.descrição_ativo
PROCESSO .Nome	ATIVO.nome_ativo
PROCESSO .Responsável	ATIVO.dono_ativo
ATIVO.Codigo	ATIVO.id_ativo
ATIVO.Codigo_tipo	ATIVO.tipo_ativo
ATIVO.Data _Descontinuado	ATIVO.data_descontinuação
ATIVO.DataAquisição	ATIVO.data_aquisição
ATIVO.Descontinuado	ATIVO.descontinuado?
ATIVO.Fabricante	ATIVO.fornecedor
ATIVO.IPAddress	ATIVO.endereço_IP
ATIVO.Nome	ATIVO.nome_ativo
ATIVO.NomeDNS	ATIVO.nome_maquina
ATIVO.NomeSoftware	ATIVO.nome_software
ATIVO.Notas	ATIVO.notas_ativo
ATIVO.Responsável	ATIVO.dono_ativo
ATIVO.SistemaOperativo	ATIVO.sistema_operativo
ATIVO.Versão	ATIVO.versão_ativo
SISTEMA_INFORMAÇÃO.Codigo	ATIVO.id_ativo
SISTEMA_INFORMAÇÃO.Codigo_tipo	ATIVO.tipo_ativo

SISTEMA_INFORMAÇÃO.HasRisk	ATIVO.possui_risco?
SISTEMA_INFORMAÇÃO.Nome	ATIVO.nome_ativo
SISTEMA_INFORMAÇÃO.Notas	ATIVO.notas_ativo
SISTEMA_INFORMAÇÃO.Responsável	ATIVO.dono_ativo
SISTEMA_INFORMAÇÃO.Risco	ATIVO.id_risco
INFORMAÇÃO.ID	ATIVO.id_ativo
INFORMAÇÃO.Descrição	ATIVO.descrição_ativo
INFORMAÇÃO.Nome	ATIVO.nome_ativo
INFORMAÇÃO.Responsável	ATIVO.dono_ativo
INFORMAÇÃO.Criticidade	INDICADOR.criticidade_indicador
INFORMAÇÃO.Classificação	INDICADOR.id_matriz_ativos_permissões
MTD.Criticidade	INDICADOR.criticidade_indicador
MTD.ID	INDICADOR.id_indicador
MTD.mtd	INDICADOR.nome_indicador
MTD.Valor	DADOS_INDICADOR.valor_indicador
RTO.Criticidade	INDICADOR.criticidade_indicador
RTO.ID	INDICADOR.id_indicador
RTO.rto	INDICADOR.nome_indicador
RTO.Valor	DADOS_INDICADOR.valor_indicador
RPO.Criticidade	INDICADOR.criticidade_indicador
RPO.ID	INDICADOR.id_indicador
RPO.rpo	INDICADOR.nome_indicador
RPO.Valor	DADOS_INDICADOR.valor_indicador
IMPACTO_IMAGEM.ID	INDICADOR.id_indicador
IMPACTO_IMAGEM.Impacto	INDICADOR.impacto_indicador
IMPACTO_IMAGEM.Valor	DADOS_INDICADOR.valor_indicador
IMPACTO_FINANCEIRO_RANGE.Days	RETIRADO POR NÃO SER UTILIZADO
IMPACTO_FINANCEIRO_RANGE.ID	RETIRADO POR NÃO SER UTILIZADO
IMPACTO_FINANCEIRO_RANGE.Value	RETIRADO POR NÃO SER UTILIZADO
IMPACTO_FINANCEIRO.ID	INDICADOR.id_indicador
IMPACTO_FINANCEIRO.Sinal	RETIRADO POR NÃO SER UTILIZADO
IMPACTO_FINANCEIRO.ValorMonetario	RETIRADO POR NÃO SER UTILIZADO
IMPACTO_FINANCEIRO.Valor	DADOS_INDICADOR.valor_indicador
HIERARQUIA_PROCESSO.Codigo	ATIVO.id_ativo
HIERARQUIA_PROCESSO.Descontinuado	ATIVO.descontinuado?
HIERARQUIA_PROCESSO.Nome	ATIVO.nome.ativo
HIERARQUIA_PROCESSO.Responsável	ATIVO.dono_ativo
CLASSIFICAÇÃO.Acesso	RETIRADO POR NÃO SER UTILIZADO
CLASSIFICAÇÃO.Controlos	RETIRADO POR NÃO SER UTILIZADO
CLASSIFICAÇÃO.Descrição	ATIVO.descrição_ativo
CLASSIFICAÇÃO.Eliminação	RETIRADO POR NÃO SER UTILIZADO
CLASSIFICAÇÃO.Exemplos	RETIRADO POR NÃO SER UTILIZADO
CLASSIFICAÇÃO.ID	MATRIZ_ATIVOS_PERMISSÕES.id_ativo
CLASSIFICAÇÃO.Marcação	RETIRADO POR NÃO SER UTILIZADO

CLASSIFICAÇÃO.Nome	MATRIZ_ATIVOS_PERMISSÕES.nome_ativo
CLASSIFICAÇÃO.Reprodução	RETIRADO POR NÃO SER UTILIZADO
CLASSIFICAÇÃO.Transmissão	RETIRADO POR NÃO SER UTILIZADO
CRITICIDADE.ID	INDICADOR.id_indicador
CRITICIDADE.Nível	INDICADOR.criticidade_indicador
CRITICIDADE.Nome	INDICADOR.nome_indicador
INTERESSADOS.Designação	INTERESSADO.nome_interessado
INTERESSADOS.Expetativa	INTERESSADO.id_expetativa
INTERESSADOS.ID	INTERESSADO.id_interessado
INTERESSADOS.ID_HPI	INTERESSADO.id_parte_interessada
PARTE_INTERESSADA.Designação	PARTE_INTERESSADA.nome_parte_interessada
PARTE_INTERESSADA.ID	PARTE_INTERESSADA.id_parte_interessada
PARTE_INTERESSADA.Observação	PARTE_INTERESSADA.observação_parte_interessada
PARTE_INTERESSADA.Order	RETIRADO POR NÃO SER UTILIZADO
EXPETATIVAS.Expetativa	EXPETATIVA.definição_expetativa
EXPETATIVAS.ID	EXPETATIVA.id_expetativa
EXPETATIVAS.ID_INTERESSADO	EXPETATIVA.id_interessado
REQUISITOS_GERAIS.Geral	REQUISITOS_GERAIS.definição_req_geral
REQUISITOS_GERAIS.ID_Requisito	REQUISITOS_GERAIS.id_req_geral
REQUISITOS_ESPECIFICOS.Designação	REQUISITOS_ESPECIFICOS.definição_req_esp
REQUISITOS_ESPECIFICOS.ID	REQUISITOS_ESPECIFICOS.id_req_esp
REQUISITOS_ESPECIFICOS.Observações	REQUISITOS_ESPECIFICOS.observações
RESPOSTA.ID_Resposta	RESPOSTA.id_resposta
RESPOSTA.Resposta	RESPOSTA.definição_resposta
TIPO_DE_ATIVOS.ARCHI_CODE	RETIRADO POR NÃO SER UTILIZADO
TIPO_DE_ATIVOS.Codigo	ATIVO.tipo_ativo_cod
TIPO_DE_ATIVOS.Exemplos	RETIRADO POR NÃO SER UTILIZADO
TIPO_DE_ATIVOS.Tipo	ATIVO.tipo_ativo
RISCO.BACKUP_OWNER_NAME	RISCO.dono_risco_backup
RISCO.ID_Num	RETIRADO POR NÃO SER UTILIZADO
RISCO.Categoria	RISCO.tipo_ativo
RISCO.ID	RISCO.id_risco
RISCO.Descrição	RISCO.descrição_risco
RISCO.Exemplos	RISCO.exemplos_risco
RISCO.Familia	RISCO.risco_dimensão
RISCO.Tipo_Categoria	RISCO.tipo_ativo_cod
RISCO.Responsável	RISCO.dono_risco
RISCO.Risco	RISCO.nome_risco
RISCO.Tipo_Risco	RISCO.risco_dimensão
RISCO.Confiencialidade	RISCO.confidencialidade?
RISCO.Disponibilidade	RISCO.disponibilidade?
RISCO.Inconformidade_ProdutosServiços	RISCO.conformidade_produtos_serviços?
RISCO.Insatisfação_ClientesParceiros	RISCO.insatisfação_clientes_parceiros?
RISCO.Integridade	RISCO.integridade?

T_RISK_ASSESSMENT.APPROVED	ANALISE_RISCO.validada?
T_RISK_ASSESSMENT.RA_COD	RETIRADO NÃO UTILIZADO
T_RISK_ASSESSMENT.RA_ENDDATE	ANALISE_RISCO.data_fim_analise
T_RISK_ASSESSMENT.RA_STARTDATE	ANALISE_RISCO.data_inicio_analise
T_RISK_ASSESSMENT.TYPE	ANALISE_RISCO.tipo_analise
T_RISK_ASSESSMENT.RA_ID	ANALISE_RISCO.id_analise
T_RISK_ASSESSMENT.RA_NAME	ANALISE_RISCO.nome_analise
T_RISK_ASSESSMENT.RA_OWNER	ANALISE_RISCO.dono_ativo
CONTROLOS.ID	CONTROLO.id_controlo
CONTROLOS.ID_CONTROL_SELECTION	CONTROLO.id_justificaçã_controlo
CONTROLOS.Nome	CONTROLO.nome_controlo
CONTROLOS.Notas	CONTROLO.notas_controlo
CONTROLOS.Número	RETIRAR NÃO UTILIZADO
CONTROLOS.Responsável	CONTROLO.dono_controlo
CONTROLOS.Justificação	RETIRADO, NÃO UTILIZADO
CONTROLOS.Evidências	CONTROLO.evidências_controlo
CONTROLOS.Categoria	CONTROLO.id_controlo_pai
CONTROLOS.BACKUP_OWNER_NAME	CONTROLO.dono_controlo_backup
CONTROLOS.Aplicavel	CONTROLO.aplicável?
CONTROLOS.Descrição	CONTROLO.descrição_controlo
LIST_CONTROL_SELECTION.ID_REASON	JUSTIFICAÇÃO_CONTROLO.id_justificação_controlo
LIST_CONTROL_SELECTION.TYPE	JUSTIFICAÇÃO_CONTROLO.tipo_justificação
LIST_CONTROL_SELECTION.Description	JUSTIFICAÇÃO_CONTROLO.descrição_justificação
CATEGORIA_CONTROLOS.Descrição	CONTROLO.descrição_controlo
CATEGORIA_CONTROLOS.ID	CONTROLO.id_controlo_filho
CATEGORIA_CONTROLOS.Nome	CONTROLO.nome_controlo
CATEGORIA_CONTROLOS.Order	RETIRADO, NÃO UTILIZADO
TRATAMENTO_RISCO.Acção	PLANO_TRATAMENTO.acção
TRATAMENTO_RISCO.Causa	PLANO_TRATAMENTO.causa
TRATAMENTO_RISCO.Controlo	PLANO_TRATAMENTO.nome_controlo
TRATAMENTO_RISCO.Custo_Estimado	PLANO_TRATAMENTO.custo_estimado
TRATAMENTO_RISCO.Data_Implementação	PLANO_TRATAMENTO.data_implementação
TRATAMENTO_RISCO.Descrição	PLANO_TRATAMENTO.descrição_plano
TRATAMENTO_RISCO.ID_Activo	PLANO_TRATAMENTO.id_ativo
TRATAMENTO_RISCO.ID_Risco	PLANO_TRATAMENTO.id_risco
TRATAMENTO_RISCO.Impacto	PLANO_TRATAMENTO.impacto_risco
TRATAMENTO_RISCO.Implementado	PLANO_TRATAMENTO.implementado?
TRATAMENTO_RISCO.Nome_Activo	PLANO_TRATAMENTO.nome_ativo
TRATAMENTO_RISCO.Nome_Risco	PLANO_TRATAMENTO.nome_risco
TRATAMENTO_RISCO.Prioridade	PLANO_TRATAMENTO.prioridade_risco
TRATAMENTO_RISCO.Probabilidade	PLANO_TRATAMENTO.probabilidade_risco
TRATAMENTO_RISCO.RA_ID	PLANO_TRATAMENTO.id_analise
TRATAMENTO_RISCO.RA_TYPE	PLANO_TRATAMENTO.tipo_risco
TRATAMENTO_RISCO.Responsável_Ativo	PLANO_TRATAMENTO.dono_ativo

TRATAMENTO_RISCO.Responsável_Risco	PLANO_TRATAMENTO.dono_risco
TRATAMENTO_RISCO.Risco_Atual	PLANO_TRATAMENTO.risco_atual
TRATAMENTO_RISCO._Estimado	PLANO_TRATAMENTO.risco_estimado
TRATAMENTO_RISCO.Tempo_Estimado	PLANO_TRATAMENTO.tempo_estimado
RESPONSÁVEL.Descrição	UTILIZADOR.função_utilizador
RESPONSÁVEL.Nome	UTILIZADOR.nome_utilizador
RESPONSÁVEL.USER_ID	UTILIZADOR.id_utilizador
USERS.ID	UTILIZADOR.id_utilizador
USERS.MAPNAME	RETIRADO, NÃO UTILIZADO
USERS.TYPE	UTILIZADOR.tipo_utilizador
USERS.USERNAME	UTILIZADOR.username

Tabela C.1: Migração de Atributos de Tabela.