Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Diretrizes para a elaboração de um Plano de Continuidade de Negócio

- Estudo de Caso -

Pedro Miguel Soares da Silva

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientador: Professor Doutor José Gaivéo

Outubro, 2016

Agradecimentos

Agradeço ao meu orientador, Professor Doutor José Gaivéo, pela orientação, experiência e conhecimento partilhado no desenvolvimento deste trabalho de dissertação.

Agradeço a todos os professores do MSIO que contribuíram para a minha aprendizagem e pelo meu sucesso neste Mestrado.

Agradeço à minha equipa de trabalho, nomeadamente ao Dr. Gil Vieira, pelas condições disponibilizadas para a frequência do Mestrado e pelo apoio no desenvolvimento do estudo de caso.

Agradeço à minha mulher Joana, por me ter acompanhado neste desafio académico, pelas ideias e pela paciência.

Agradeço aos meus colegas do MSIO, pela amizade e experiência partilhada.

E agradeço a todos que, direta ou indiretamente, fizeram parte desta experiência.

Índice

Índice de Figuras:

Índice de Tabelas:

Lista de Siglas

AMA – Agência para a Modernização Administrativa

BCM – *Business Continuity Management*

BCP – *Business Continuity Plan*

BIA - *Business Impact Analysis*

BGP – Border Gateway Protocol

CD – Conselho Diretivo

CMD – *Change Management Database*

COBIT – *Control Objectives for Information and Related Technology*

DRP – *Disaster Recovery Plan*

EAMS – *Enterprise Architecture Management System*

ERD – Equipa de Recuperação de Desastre

ERI – Equipa de Resposta a Incidentes

IRM – *Institute of Risk Management*

ISACA – *Information Systems Audit and Control Association*

ISO – *International Organization for Standardization*

IT – *Information Technology*

ITIL – *Information Technology Infrastructure Library*

MTD – *Maximum Tolerable Downtime*

PDCA – *Plan, Do, Check, Act/Adjust*

PGETIC – Plano Global Estratégico para a Racionalização e Redução de Custos com as Tecnologias de Informação e Comunicação

PGPRIC - Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

RPO – *Recovery Point Objective*

RTO – *Recovery Time Objective*

SAN – *Storage Area Network*

SGSI – Sistema de Gestão da Segurança da Informação

SI – Sistemas de Informação

SLA – *Service Level Agreement*

TIC – Tecnologias de Informação e Comunicação

WRT – *Work Recovery Time*

Resumo

As organizações estão sujeitas regularmente a desastres naturais e outras situações que causam disrupções e indisponibilidade no seu negócio. Torna-se necessário a existência de uma política de gestão de risco e de continuidade que auxilie as organizações a minimizar esses riscos. Este documento identifica as diretrizes necessárias para a elaboração de um plano de continuidade do negócio, suportado por um plano de recuperação. O estudo apresenta uma metodologia de desenvolvimento de um plano de continuidade, devidamente suportado por um estudo de caso que demonstra a elaboração desse plano numa organização. O objeto desse estudo de caso é um plano de continuidade e recuperação de acordo com as diretrizes identificadas, sendo desenvolvida uma metodologia, identificados os riscos e os sistemas críticos do negócio, e definida uma estratégia de continuidade e recuperação. A investigação demonstra a importância dessas políticas de gestão e dos respetivos planos em qualquer organização, devidamente alinhados com o negócio e mantidos ao longo do tempo.

Palavras-chave: *Business Continuity*, *Disaster Recovery*, Segurança da Informação, Sistemas de Informação, Risco.

1. Introdução

Vivemos numa sociedade dominada por organizações, grandes ou pequenas, com ou sem fins lucrativos nas quais as pessoas trabalham em conjunto, com vista à prossecução de objetivos (Teixeira, 2005).

A informação é um dos seus principais recursos, podendo ser definida como um conjunto de dados colocados num contexto útil e de grande significado (Varajão, 2005), útil para responder às exigências do mercado e da globalização de forma a garantir uma vantagem competitiva. Para gerir a informação e tomar as decisões corretas, a organização recorre aos Sistemas de Informação (SI), não só pela facilidade de agregação de dados, mas também pelo valor e conhecimento que o negócio pode extrair dessa mesma informação de forma sistematizada. Por outras palavras, é um conjunto de meios e procedimentos cuja finalidade é assegurar a informação útil necessária às diversas funções e níveis da organização, bem como à sua envolvente externa (Varajão, 2005).

Devido exatamente a essa envolvência, a organização encontra-se exposta a diversos tipos de ameaças que podem causar impacto no seu negócio e até de outras organizações clientes, parceiras e/ou fornecedoras de serviços. Nesse sentido, torna-se pertinente a existência de um plano que expresse a forma como garantir o cumprimento da missão e dos objetivos a que a organização se propôs, de modo a preservar a sua personalidade jurídica e assegurar a continuidade do negócio em caso de disrupção.

Há vários tipos de planos. Há planos que são guias de orientação permanente por períodos mais ou menos longos. São as políticas, os procedimentos e os regulamentos (Teixeira, 2005). Podem existir em qualquer nível do planeamento, nomeadamente relativos à recuperação financeira, de recursos humanos e da infraestrutura tecnológica que suportam os SI das organizações.

No entanto, um plano mal elaborado ou não atualizado pode comprometer a recuperação do negócio e da organização, bem como a segurança da informação na sua integridade, confiabilidade e disponibilidade. Torna-se evidente a existência de um plano de continuidade de negócio, comumente referido pelo termo em inglês *Business*

Continuity Plan (BCP), devidamente elaborado de acordo com os *standards*[1] e linhas orientadoras gerais.

Muitas organizações subestimam a existência desses planos, seja por razões financeiras ou desconhecimento. A continuidade de negócio está integrada com a gestão do risco, na sua vertente mais operacional. É um desafio que as organizações têm de lidar, em antecipar os acontecimentos inesperados, prevenir e mitigar esses riscos.

1.1. Objetivo

A gestão do risco e a continuidade do negócio tem um papel fundamental nas organizações de hoje em dia, tanto privadas como públicas, garantindo a sua sobrevivência e competitividade no mercado em que se encontram.

O objetivo principal deste documento é a identificação de diretrizes, elencando *standards* internacionais e boas práticas de gestão de serviços das Tecnologias de Informação e de *governance*, que servem de referência para a elaboração de um BCP, demonstrado pelo estudo de caso.

As organizações estão cada vez mais dependentes dos SI, pelo que o desenvolvimento deste BCP é orientado à recuperação da infraestrutura tecnológica, através de mecanismos de substituição ou replicação, permitindo uma recuperação total dos processos de negócio e dados dentro de uma janela temporal adequada. Este tipo de plano de recuperação e continuidade é conhecido por *Disaster Recovery Plan* (DRP).

1.2. Problemática

A dependência das tecnologias é cada vez maior tal como as ameaças a que estão sujeitas. Conhecer os problemas potencialmente provocados por falhas e desastres, as soluções que existem para evitar esses riscos ou recuperar a infraestrutura tecnológica após um evento, assim como o custo associado, torna-se imprescindível a todos os interessados, desde a gestão de topo aos utilizadores, aos parceiros e aos clientes, que querem garantir a continuidade do seu negócio e no mais curto espaço de tempo.

Em todas as organizações deve existir um plano de continuidade para o caso de uma falha disruptiva, contemplando uma solução adequada ao negócio e compatível com

[1] Padrão ou norma. Visa predefinir regras no desenvolvimento de, neste caso, planos de continuidade.

as restrições financeiras e legais. Um BCP pode ser muitas vezes oneroso, não só pela sua elaboração e eventual certificação, mas também pelos custos físicos de equipamentos e locais de instalação alternativos (quando suportado por um DRP), sejam eles um serviço de *housing*[2], *hosting*[3] ou próprio (caso seja multipolar e de elevada dimensão). Um exemplo simples: é hoje fundamental para qualquer nível de *tier*[4], o armazenamento de *backups*[5] *off-site*, em local seguro afastado do centro de dados bem como um local alternativo para restaurar essa informação guardada.

1.3. Estrutura do Documento

O presente documento encontra-se dividido em sete capítulos.

Neste capítulo, introduz-se a dependência tecnológica por parte das Organizações e os problemas associados, bem como o objetivo, metodologia e a pertinência do tema.

No segundo (Enquadramento Teórico) pretende-se fazer uma breve revisão bibliográfica de alguns conceitos teóricos essenciais à compreensão do estudo empírico a realizar, com a introdução das diretrizes internacionais para a Continuidade de Negócio, Gestão de Risco e elaboração de planos de recuperação, e as boas práticas de gestão de serviços de tecnologias de informação.

O terceiro capítulo, Caracterização da Organização, descreve a organização que serve o estudo de caso empírico seguido do quarto capítulo, Caracterização do Problema, que identifica a problemática relacionada com o tema.

O capítulo Apresentação do Estudo de Caso, descreve a metodologia usada pela organização para a elaboração do BCP, com destaque de algumas *frameworks*[6] e ferramentas de desenvolvimento.

O capítulo sexto, Resultados, constitui um registo das atividades e análise dos resultados obtidos na construção desse plano.

[2] Modalidade de alojamento partilhado de equipamentos físicos, por exemplo infraestruturas tecnológicas.

[3] Modalidade de alojamento partilhado de sistemas de informação, nomeadamente servidores virtuais.

[4] Categorização por níveis. Neste caso, camadas de dados alvo de cópias de segurança que variam com a sua importância e acessos.

[5] Cópia de segurança de dados.

[6] Entende-se como uma estrutura de suposições, conceitos, valores e práticas, usada na construção de algo.

Por fim, a Conclusão com uma reflexão sobre o tema e Perspetivas de Trabalho Futuro da continuidade de negócio da organização alvo de estudo.

1.4. Metodologia

A abordagem utilizada neste estudo é qualitativa e o método escolhido para obtenção dos dados necessários à validação do tema, um estudo de caso que decorrerá numa organização.

Foi realizado uma investigação sobre as melhores práticas e normas de gestão de continuidade de negócio, tendo sido identificado diretrizes consideradas adequadas à elaboração de um plano.

É feito um enquadramento teórico no sentido de descrever as propriedades e características das diretrizes mais relevantes para a elaboração de um plano, e posteriormente correlacionado com o estudo de caso de forma a avaliar a relação entre conceitos e orientações recolhidas durante essa investigação.

O estudo de caso reflete a elaboração de um plano de continuidade, sendo feito uma análise crítica validando se o seu desenvolvimento respeitou as diretrizes identificadas, se são aplicáveis e suficientes.

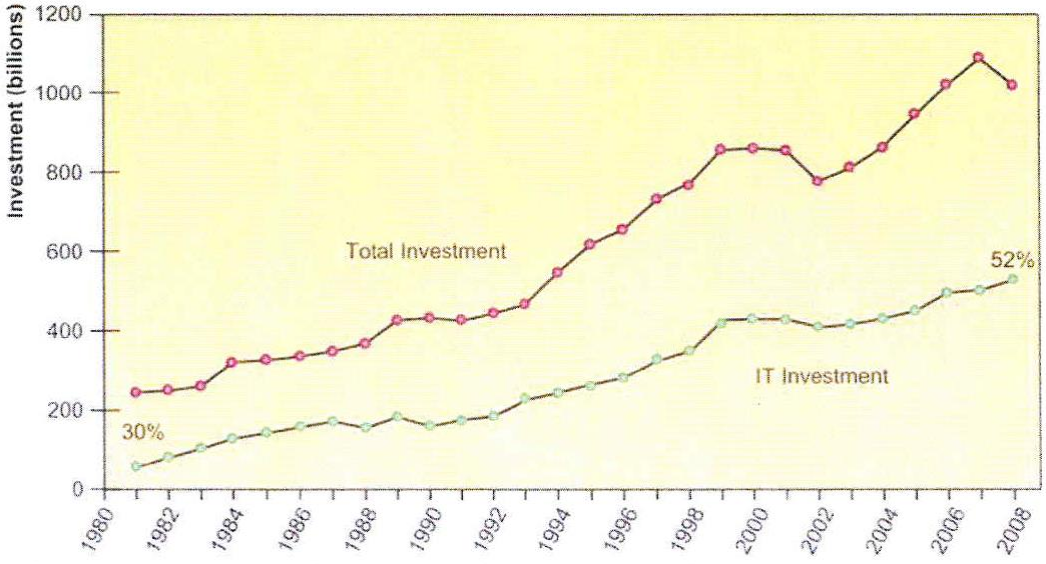
2. Enquadramento Teórico

Neste capítulo desenvolveu-se o trabalho de revisão bibliográfica relativo ao tema, de forma a construir a estrutura teórica do estudo de caso. Recorreu-se especialmente a *standards* internacionais e *frameworks* desenvolvidas por entidades de normalização e boas práticas.

Encontra-se estruturado em cinco subcapítulos de modo a enquadrar a necessidade de continuidade de negócio e dos respetivos planos que a suportam, identificar as *frameworks* mais comuns, bem como os *standards* tidos como relevantes para o planeamento de um BCP, a perspetiva holística do *Business Continuity Management* (BCM) e a metodologia recomendada para a elaboração de um BCP, que serve de base ao estudo de caso apresentado no capítulo 5.

2.1. As Organizações e a continuidade de negócio

É possível verificar a importância das tecnologias nas organizações, sejam elas públicas ou privadas, nos últimos anos, de acordo com a figura 1. Os SI têm transformado as organizações, as pessoas e os processos de negócio. Tem igualmente reduzido as distâncias e esvanecendo as fronteiras, aproximando culturas e economias distantes – globalização – bem como levando a uma disseminação de conhecimento.



Information technology capital investment, defined as hardware, software, and communications equipment, grew from 32 percent to 52 percent of all invested capital between 1980 and 2009.

Source: Based on data in U.S. Department of Commerce, Bureau of Economic Analysis, *National Income and Product Accounts*, 2009.

Figura 1 – Capital investido nas TIC norte americanas de 1980 a 2008.
(Laudon & Laudon, 2012)

O economista Fritz Machlup foi um dos primeiros estudiosos a introduzir o conceito da Sociedade da Informação, como uma organização que dependia do conhecimento (valor extraído da informação) e este dos fatores ambientais, internos e externos à organização (Crawford, 1983).

Consequentemente, as organizações defrontam-se com algumas dificuldades como fraquezas ou falhas que expõe ativos[7] de informação a ataques ou danos. Assim, encontra-se sujeita a eventos que podem conduzir a danos potenciais e causar efeitos indesejáveis – ameaça - aos ativos identificados como fundamentais para a sua atividade.

A probabilidade de uma determinada ameaça explorar uma vulnerabilidade particular levou a uma crescente atenção sobre o risco. Esta preocupação deriva do interesse dos atuais e potenciais investidores nas organizações, em obterem informação de qualidade que lhes possibilitem tomar decisões de carácter económico e financeiro. A sua avaliação e gestão afeta o desempenho e a *performance* económica futura das organizações com menor risco e mais certezas (Dobler, 2005).

É atualmente possível encontrar normas que abrangem determinadas componentes do risco visto que a sua gestão possibilita maior esclarecimento às organizações e diminui as incertezas no negócio e no mundo financeiro.

As organizações não só dependem uma das outras como só conseguem sobreviver se adicionarem valor às suas atividades e à dos vários intervenientes. Ao viverem num ecossistema em que a sobrevivência depende das estratégias certas e dos modelos adequados a cada negócio e da sua relação com o ambiente, é necessário garantir a sua continuidade de modo a atingir os objetivos a que se propôs.

As organizações sensibilizadas para a importância da gestão do risco têm muitas soluções teóricas e empíricas que podem adotar, dependendo da sua estrutura organizacional, dimensão, mercado e fatores ambientais (legais, financeiros, clientes, fornecedores, entre outros). O sistema de gestão de risco deve ser definido de acordo com a maturidade e expectativas que a organização tem do risco (IRM, 2002).

De acordo com o s*tandard* de Gestão de Risco do *Institute of Risk Management* (IRM) a avaliação do risco permite identificar, categorizar o risco e estimar a probabilidade de ocorrência bem como a consequência do impacto na organização. É avaliado de acordo com os critérios estabelecidos pela organização tendo em conta fatores

[7] Entende-se por ativo como um recurso importante, neste caso para a organização.

custo-benefício, restrições legais, fatores económico-sociais e ambientais, interesses dos *stakeholders*, entre outros. A análise final serve para alertar a organização dos riscos existentes e a forma como cada um deve ser tratado ou aceite.

Existem inúmeras ações de tratamento que permitem a sua mitigação, atenuação, transferência ou exploração (além da sua aceitação como indicado anteriormente) dos impactos decorrentes de um risco a que uma organização está exposta: medidas proactivas (desencadeadas *a priori* de um evento) e medidas reativas (desencadeadas *a posteriori* de um evento, sendo só possível através de um planeamento antecipado).

Nenhuma organização tem controlo absoluto sobre a envolvente onde se encontra, nem em nenhum instante temporal pode enfrentar um evento anómalo que ameace a sua atividade. Torna-se assim essencial assegurar a continuidade do negócio face à ocorrência dessas tais situações anómalas, através da prevenção da sua ocorrência, diminuição do impacto provocado e garantindo que os processos de negócio são recuperados de acordo com o estabelecido pela organização como serviços mínimos e minimizando as perdas.

Mas qual é o objetivo? Um BCP, para além de garantir a continuidade do negócio em caso de uma disrupção, protege os interesses, bens e conhecimento da organização, permite cumprir imperativos legais e contratuais, minimizar impacto junto dos seus clientes, fornecedores e parceiros bem como protege a sua imagem. Permite a identificação de riscos e providencia a base de trabalho e dota a organização de mecanismos necessários para responder de uma forma coordenada a desastres com impacto nas atividades críticas do negócio.

Entenda-se por desastre um evento repentino com um impacto significativo, que origina uma disrupção por um período de tempo superior ao tolerado pelo negócio. O incidente é um evento com potencial para tornar-se um desastre, o qual deve ser analisado de forma a tomar-se medidas adequadas.

A continuidade de negócio é um processo estratégico e transversal a toda a organização, focada principalmente nos processos de negócio, mas tendo em consideração as sinergias e dependências com as pessoas, tecnologias e outros recursos. Ou seja, deve estar alinhada com os objetivos, estratégias do negócio e dimensão da organização.

A gestão da continuidade de negócio deve assegurar o desenvolvimento, a implementação, a manutenção e a integração de planos adequados à prossecução dos

objetivos da organização, podendo ser planos de segurança física e da informação, planos de contingência, planos de comunicação, planos de negócio e planos de recuperação. Este último plano, o DRP, é uma das dimensões mais comuns e importantes na elaboração de um BCP, na medida que garante a recuperação de uma disrupção dos Sistemas de Informação/Tecnologias de Informação e Comunicação (SI/TIC) de uma organização.

Um dos maiores riscos que pode afetar a continuidade do negócio de uma organização é a desatualização do respetivo plano. Este deve ser alvo de melhoria contínua, de forma a contemplar as alterações que, entretanto, ocorreram e que possam colocar em causa a capacidade de resposta desse mesmo plano.

A realização de testes e uma monitorização contínua deve estar inserida num ciclo contínuo de verificações e correção de anomalias, que assegure a permanente adequação do plano aos requisitos de continuidade da organização.

2.2. *Frameworks* e boas práticas

Neste documento tem sido feito muitas referências aos Sistemas de Informação e a sua relação simbiótica com uma organização.

Sendo um sistema um agregado de elementos simples ou complexos que interagem entre si de modo a acrescentar novas funcionalidades ao conjunto, que não existem nos elementos isolados (Caetano, 2013), um SI é um conjunto de ideias que organizam e tratam a informação de forma automática ou não, e que interagem com outros sistemas[8], geralmente de informação e a organização. São produtos desenvolvidos de acordo com planos e especificações em que o seu sucesso mede-se pela conformidade com os requisitos e pelo impacto global na organização. São igualmente produtos que fazem parte do ecossistema da organização sujeitos à envolvência ambiental e riscos associados.

O alinhamento entre as tecnologias e o negócio é constante, já que compete aos SI estar permanentemente em mudança para se adaptar ao contexto de mudança acelerada do negócio.

Mas como se pode definir e desenhar o SI ideal para a organização?

[8] Um sistema é um conjunto de atores e todos os elementos a estes associados que partilham objetivos e/ou princípios comuns.

Para ajudar a definir todos os artefactos[9] e componentes de um SI, temos um *standard* internacional, o ISO 42010:2011 devidamente integrado no COBIT 5[10] e no ITIL v3[11], *frameworks* de *governance* e boas práticas de gestão de serviços TIC respetivamente.

O ISO 42010 define os requisitos para a designação do sistema, *software* e arquiteturas empresariais[12]. Tem como objetivo padronizar a prática da arquitetura e conceitos, apresentando uma base conceptual para desenhar, comunicar e rever arquiteturas da informação, tecnológicas, aplicacionais e de processos bem como a especificação de requisitos.

Em conjunto, estas arquiteturas e *frameworks* garantem que uma organização atende às necessidades dos *stakehoders*, alinha os SI/TIC com o negócio, integra todos os componentes de uma organização, promove a segurança, traz integridade e consistência dos dados, e reduz a duplicação e o custo-efetivo.

O COBIT 5 está dividido em duas partes, uma para *governance* e outra para Gestão de TI da organização, de acordo com a figura 2 que representa a sua família de produtos.

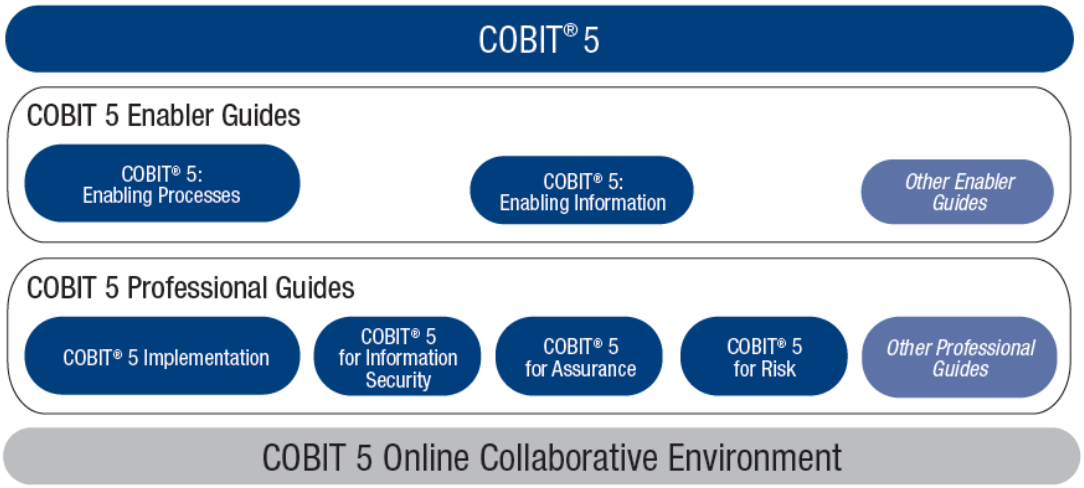


Figura 2 – Familia de produtos do COBIT 5

(ISACA, 2012)

[9] Entende-se por artefacto, objetos diversos que incluem pessoas, estratégias, processos de negócio, SI e tecnologias.

[10] *Control Objectives for Information and Related Technology*

[11] *Information Technology Infrastruture Library*

[12] De acordo com o ISO 42010:2011, é um conjunto de princípios coerentes e consistentes que guiam o desenho, engenharia e a concretização de uma organização.

Governance (representando pelos *Enable Guides*) garante que as necessidades, condições e opções dos *stakeholders* sejam avaliadas a fim de determinar os objetivos organizacionais, definindo a estratégia através de prioridades e tomadas de decisão, monitorizando o desempenho e a conformidade com os objetivos estabelecidos.

A *Information Systems Audit and Control Association* (ISACA), entidade responsável pelo COBIT 5, desenvolveu um manual para a aplicação dos modelos de *governance*, através de um recurso para profissionais composto por guias (*Professional Guides*) de Segurança da Informação, *Assurance* e (Gestão de) Risco, representado pelos Guias Profissionais na família de produtos do COBIT.

O COBIT 5, como modelo de *governance*, foca-se mais nos controlos e nas métricas e não tanto na segurança, mas releva a importância e o impacto do risco para a organização, orienta o apetite ao risco, define uma cultura de risco e quantifica os ativos sujeitos a risco de forma a contabilizar os custos de mitigação ou perdas em caso de exposição. Por isso, o COBIT 5 encontra-se em sintonia com os *standards* internacionais ISO 31000 - *Risk Management*, ISO 27005 – *Information technology – Security techniques - Information Security Risk Management* e COSO – *Enterprise Risk Management*, de modo a assegurar que as necessidades de segurança da organização estão alinhadas com o negócio e tecnologias que as suportam.

Sumariamente, o ISO 31000 estabelece princípios e orientações genéricas sobre a gestão de risco. O ISO 27005 é constituído pelas definições dos processos de gestão de riscos de segurança de informação e pelas suas atividades. Enquanto que o COSO é uma *framework* integrada que inclui os métodos e processos utilizados pelas organizações para gerir os riscos e aproveitar as oportunidades relacionadas com a prossecução dos seus objetivos.

No entanto, o ITIL v3 é uma abordagem para a gestão de serviços de TI melhor aceite em todo o mundo. Fornece um conjunto coerente de boas práticas, provenientes dos sectores público e privado a nível internacional. Defende que as tecnologias devem estar alinhadas com as necessidades do negócio e apoiar os processos centrais de negócio. Fornece orientações para as organizações sobre como usar os SI como uma ferramenta para facilitar a mudança, transformação e crescimento dos negócios, incluindo a segurança.

As melhores práticas do ITIL v3 são atualmente detalhadas em cinco publicações, conforme representado pela figura 3, que fornecem uma abordagem sistemática e profissional para a gestão das TIC, permitindo às organizações prestar serviços adequados e garantir continuamente que esses serviços estão a alinhados com a estratégia do negócio, beneficiando todos os seus utilizadores.

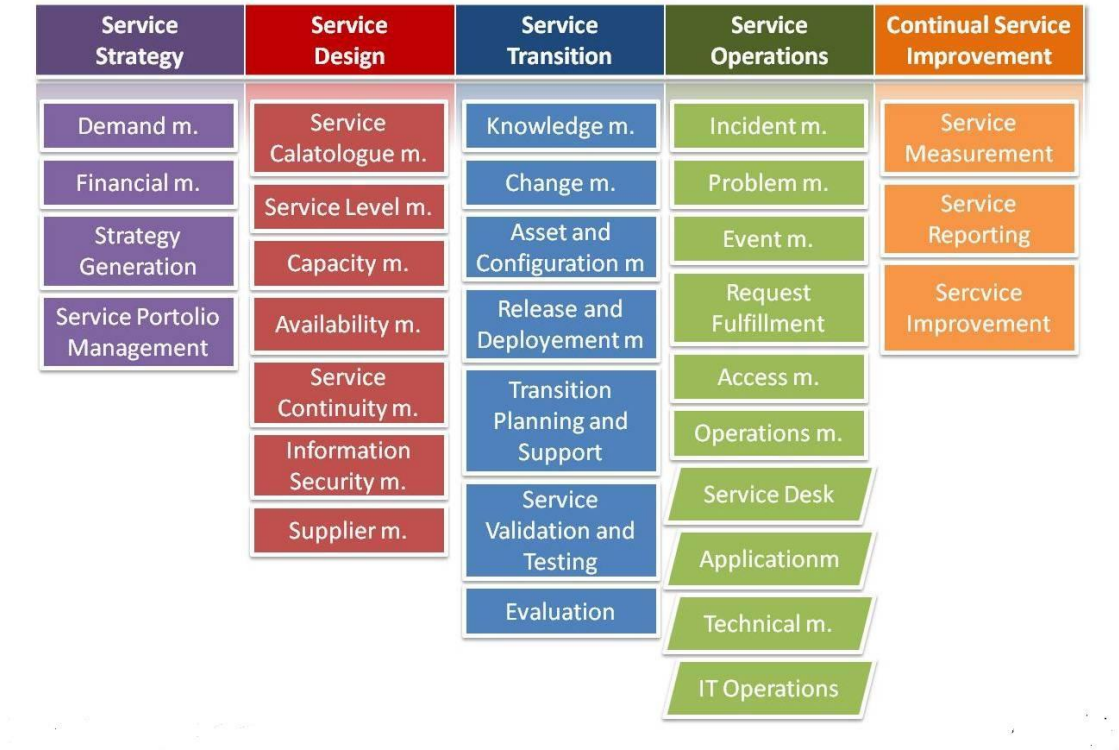


Figura 3 – *Framework* ITIL v3
(Mundo ITIL, 2016)

Da publicação *Service Design*, que tem o intuito de fornecer as boas práticas de desenho/desenvolvimento de gestão de serviços de Tecnologias de Informação[13] e respetivos processos, destacam-se os processos de *Information Security Management* e *Service Continuity Management*.

O processo de *Information Security Management*, descreve a estrutura de segurança da informação na gestão da organização e baseia-se no ISO 27001. Tem como objetivo garantir que os métodos e procedimentos *standard* são utilizados para um tratamento eficiente e imediato de todas as questões relacionadas com segurança e a

[13] Comumente conhecido pelo termo inglês *information technology – IT.*

identificação e seguimento de todo e qualquer privilégio de acesso seguro à organização (ITSMF, 2010), e que garanta a continuidade de negócio.

Já o processo *Service Continuity Management* suporta o processo global de continuidade da organização e respetiva recuperação de desastres, bem como outros planos de resiliência. Matematicamente, pode-se considerar este processo como um "subconjunto" do BCP.

Como indicado anteriormente, a organização é dinâmica e encontra-se em constante transformação de modo a adaptar-se ao mercado e ao ambiente que a rodeia, pelo que é necessário acompanhar o impacto, o custo ou o benefício do risco dessa alteração, a sua disponibilidade, continuidade e mudança, a monitorização, a implementação e os pedidos de alteração.

Como é possível validar, ambas as *frameworks* não são dedicadas à segurança da informação, mas complementam-se com os *standards* de forma a determinar e melhorar a postura de segurança da organização.

Apesar de não ser referenciada, o ISO 20000 – *Information Technology – Service Management*, contempla processos alinhados com os do ITIL. Tal como esta *framework*, é um conjunto de boas práticas de gestão de serviços IT. A figura 4 demonstra essa relação entre o ITIL, o *standard* e a sua importância na gestão de serviços IT.

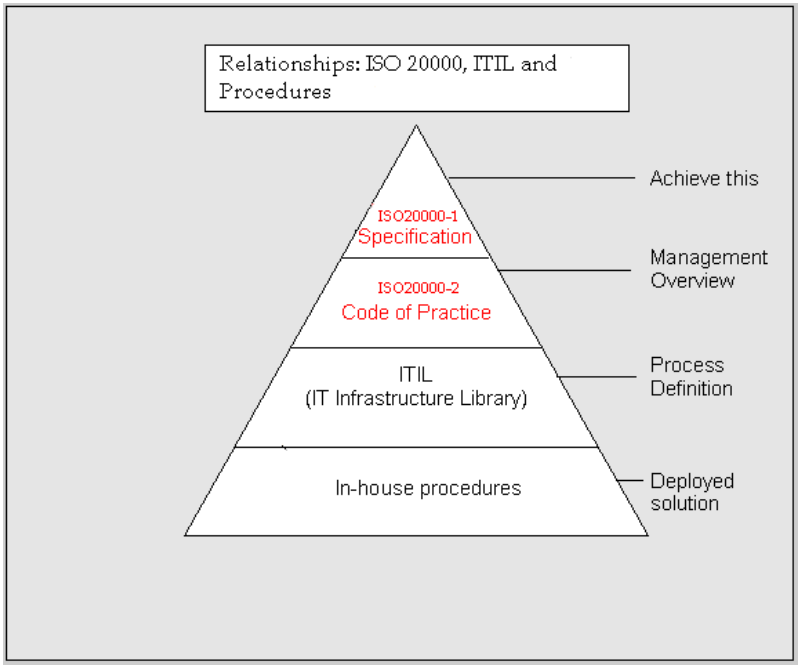


Figura 4 – O Triângulo do ITIL
(ITIL and ITSM World, 2005)

O ISO 20000 segue a metodologia *Plan, Do, Check, Act/Adjust* (PDCA) para garantir uma prestação de serviços de qualidade, através de ajustes e verificações que visam a melhoria contínua dos processos. Encontra-se igualmente alinhada com o ISO 9000 – *Quality Management* e o ISO 27001. Esta metodologia é comum na gestão de serviços, como nos planos de continuidade e nos *standards* internacionais.

2.3. *Standards* Internacionais

A gestão da continuidade do negócio, tal como qualquer outra política de gestão de uma organização, é mais eficaz e eficiente quando fundamentada em normas internacionais e orientada aos objetivos do negócio. Este alinhamento confere a credibilidade e a viabilidade de um BCP.

É possível verificar no subcapítulo anterior, a estreita relação entre as *frameworks* de gestão de serviços e *governance* com os *standards* internacionais.

No entanto, o que é um *standard*? Para que serve? Qual a sua importância num plano? O que está em causa?

Os *standards* internacionais são normas, padrões, códigos de conduta internacionalmente aceites. Elaborados pela *International Organization for Standardization*, tanto a organização como as normas, são conhecidos por ISO[14]. Esta abreviatura tem origem na palavra grega ἴσος (isos) que significa igualdade, com valor similar. Ou seja, de acordo com a própria ISO.org, o ISO é um documento que contém informação prática e boas práticas, sendo muitas vezes descrito como uma maneira de fazer as coisas ou uma resolução para um problema global acordado por todos. De uma forma resumida, o ISO torna os produtos compatíveis, identifica *issues* de segurança de produtos e serviços, partilha ideias e soluções, *know-how* tecnológico e as melhores práticas de gestão. Exemplos do nosso dia-a-dia da presença dos *standards*, são o câmbio e a moeda, os cartões de crédito, códigos dos países, entre outros.

Os *standards* são desenvolvidos para responder a uma situação específica existente do mercado e elaborados por pessoas que sentem essa necessidade de normalizar os procedimentos. Essas necessidades são depois identificadas, adequadas aos vários países e compiladas pela ISO.org.

[14] Devido ao uso da mesma sigla, a organização é identificada neste documento por ISO.org e o *standard* por apenas ISO.

No entanto, são as organizações que podem extrair os maiores benefícios dos *standards*. Estes servem exatamente para garantir a *compliance* dos processos e procedimentos para resolver situações específicas, que no âmbito deste documento referem-se à continuidade do negócio e respetiva recuperação.

O desenvolvimento de um BCP, com origem na gestão da continuidade e da disponibilidade da informação de uma organização, tem em conta as boas práticas e normas de segurança da informação além dos *standards* específicos para a sua elaboração e diretrizes de adequação das TIC para a continuidade do negócio.

Quer-se com isto dizer que, sendo a informação o ativo mais precioso da organização, para o seu sucesso e cumprimento dos objetivos a que se propôs, e de forma a garantir a continuidade do negócio em caso de disrupção (neste caso das SI/TIC que a suportam), é necessário que a informação esteja disponível quando solicitada pelos interessados e devidamente autorizados (confidencialidade), de forma completa e íntegra, autêntica e não repudiável (troca de informação de forma confiável). A segurança da informação deve ser tratada pela organização de uma forma preventiva e não somente após um evento disruptivo.

Neste sentido, de forma a garantir a continuidade, a Segurança da Informação serve para reduzir os custos decorrentes da ocorrência de incidentes ou mesmo a necessidade de garantir a conformidade legal de atividades organizacionais.

Na sequência do uso de *frameworks* de gestão de serviços e *governance*, nomeadamente das publicações referentes à Gestão da Segurança e do Risco, a utilização do ISO 27001 bem como do ISO 31000, proporciona um enquadramento relevante para a continuidade do negócio e de todas as suas atividades, possibilitando igualmente a articulação com outros *standards*, de forma a implementar um sistema de segurança da informação nas organizações.

O ISO 27001 estabelece os requisitos para o sistema de gestão da segurança da informação (SGSI). Juntamente com os restantes ISO da família 27000 (ISO27k), a organização consegue gerir a segurança dos seus ativos, tal como a informação financeira, propriedade intelectual, informação dos seus recursos ou dos seus parceiros. De acordo com a ITSMF (Portugal), garante que os métodos e procedimentos *standard* são utilizados para um tratamento eficiente e imediato de todas as questões relacionadas com

segurança e a identificação e seguimento de todo e qualquer privilégio de acesso seguro à organização e sua informação.

Como qualquer outro *standard* de sistemas de gestão a certificação é possível, mas não é obrigatória. Algumas organizações escolhem implementar os *standards* para beneficiar das melhores práticas, enquanto outras decidem pela certificação por questões de imagem, garantindo aos seus clientes e parceiros que respondem às recomendações internacionais. É possível verificar na figura 5 a distribuição de certificações ISO 27001, a relevância que este *standard* tem nas organizações a nível mundial e a importância da segurança da informação.

Figura 5 – Distribuição mundial de certificações ISO 27001 em 2014
(ISO, 2014)

No caso de Portugal, a importância do SGSI tem crescido de forma linear, demonstrando a preocupação com a segurança da informação e do risco a que a organização está sujeita, bem como a importância da imagem que esta tem perante os clientes, parceiros e mercado onde está inserida, conforme representado na figura 6.

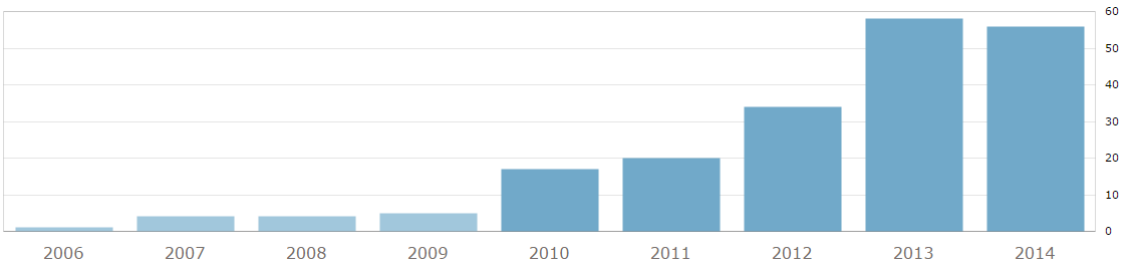


Figura 6 – Distribuição de Certificações ISO 27001 em Portugal
(ISO, 2014)

O SGSI é usado pela organização para identificar, analisar e endereçar os riscos da informação. Garante igualmente um ajuste dinâmico dos *standards* e boas práticas às mudanças das ameaças, vulnerabilidades e impactos que estas têm no negócio.

Mas o ISO 27001 não formaliza controlos específicos de segurança pois estes dependem da organização, do negócio e dos riscos a que estão sujeitos. Complementada pelo ISO 27002 – *Information Technology – Security Techniques – Code of Pratice for Information Security Tools*, que disponibiliza orientações para as normas de segurança da informação organizacionais e práticas de gestão de segurança da informação, incluindo a seleção, implementação e gestão de controlos tendo em consideração o ambiente de risco da organização. Este *standard* foi desenhado para ser usado pelas organizações que pretendem controlos específicos durante um processo de implementação de um SGSI com base no ISO 27001, implementar controlos de segurança da informação mundialmente aceites e desenvolver as suas próprias diretrizes de segurança da informação (IsecT Ltd, 2016).

No entanto, quando se pretende efetuar a gestão do risco no âmbito da segurança da informação, deve-se usar o ISO 27005 – *Information Technology – Security Techniques – Information Security Risk Management*.

Os *standards* ISO27k são desenhados deliberadamente alinhadas com o risco, ou seja, as organizações são incentivadas a avaliar os riscos da segurança da informação como uma ação preliminar para tratá-los de várias maneiras.

O ISO 27005 não especifica, recomenda ou indica qualquer método de gestão de risco. Implica, no entanto, um processo contínuo e sequencial estruturado de atividades. Estas consistem na definição do contexto de gestão de risco (âmbito das conformidades, métodos e políticas, tolerância ao risco ou apetite); analisar e avaliar o risco tendo em conta os ativos de informação, ameaças, controlos e vulnerabilidades existentes para determinar a probabilidade de incidentes ou eventos, e as consequências/impactos previstos de forma a determinar o nível de risco; mitigar, aceitar, evitar ou transferir os riscos de forma adequada e com a prioridade devida; informar todos os interessados durante o processo e monitorizar, identificar, avaliar, tratar e agir adequadamente às mudanças significativas.

Por sua vez, existe outro *standard* "padrão" para a gestão de risco, devido essencialmente ao seu contexto generalista aplicável a qualquer área de gestão de risco (finanças, engenharia, entre outras): trata-se do ISO 31000. Embora a maioria das organizações já possua uma metodologia de gestão de riscos, esta norma define um conjunto de princípios que assegura a sua eficácia. Sugere igualmente que as organizações desenvolvam, implementem e melhorem essa metodologia, cujo objetivo é integrar o processo de gestão de risco na *governance*, estratégia e planeamento, bem como na gestão, comunicação de dados e resultados, políticas, valores e cultura da organização.

Riscos que afetam as organizações podem ter consequências em termos de desempenho económico e reputação profissional, bem como do meio ambiente, segurança e resultados sociais. A gestão do risco efetivamente ajuda as organizações a um bom desempenho num mercado cheio de incertezas.

No entanto, o risco está sempre presente e os incidentes e eventos disruptivos associados podem afetar a continuidade (incluindo a segurança) de funções críticas do negócio tal como a sua operação. Na família ISO27k, existe outro *standard* que descreve os conceitos e princípios, fornece uma estrutura de métodos e processos que identificam e especificam todos os aspetos de desempenho, desenho e implementação para melhorar a resposta das TIC de uma organização de forma a garantir a continuidade do negócio: ISO 27031 – *Information technology -- Security techniques -- Guidelines for Information and Communication Technology Readiness for Business Continuity*.

Estas linhas orientadoras aplicam-se a qualquer organização, desenvolvendo a disponibilidade das TIC na gestão da continuidade e exigindo infraestruturas tecnológicas capazes de apoiar o negócio durante esses eventos disruptivos não planeados. Ao assegurar a resiliência das TIC, é possível recuperar dentro de prazos tidos como necessários e devidamente acordados pela organização a níveis de serviço pré-determinados, que garantam a continuidade do negócio.

Todos estes *standards* têm como objetivo disponibilizar normas, boas práticas, metodologias e controlos que permitem um tratamento eficiente e imediato de todas as questões relacionadas com a segurança, que otimiza a capacidade da infraestrutura tecnológica e ajuda a organização a oferecer um nível sustentado a um custo aceitável de disponibilidade, e que suporta o processo global de gestão de continuidade da

organização, garantindo a recuperação das instalações e das TIC, dentro de prazos requeridos e acordados.

2.4. *Business Continuity Management*

É sobre exatamente a elaboração de planos e recuperação das infraestruturas tecnológicas e o que é necessário para garantir a continuidade do negócio que este subcapítulo se foca, com base nas *frameworks* e *standards* já introduzidos anteriormente e noutros de igual ou maior relevância para a elaboração de um BCP.

Como tem sido possível verificar, a tecnologia é, sem dúvida, a base dos processos de negócio, da continuidade, da disponibilidade e da sobrevivência de qualquer organização nos dias de hoje.

A necessidade de planos de contingência e recuperação de desastres das tecnologias, surgiram com as catástrofes naturais e terrorismo durante os anos 1980 e início de 1990. Houve um reconhecimento cada vez maior do impacto das tecnologias nos processos de negócio e as interrupções a que as organizações estariam sujeitas no caso de um evento. A disciplina tornou-se então conhecida como *Business Continuity Management (BCM)* (Gasiorowski-Denis, 2012).

Tanto os governos como entidades reguladoras, começaram a reconhecer o papel da gestão de continuidade de negócios na mitigação dos efeitos de incidentes perturbadores sobre a sociedade, procurando obter a garantia de que as organizações privilegiassem esta gestão. As próprias organizações, reconheceram a sua dependência em relação aos seus fornecedores e parceiros, bem como a necessidade de garantir a prestação de serviços mesmo quando estes eventos disruptivos ocorrerem. Isto é conseguido através da introdução de medidas de redução de risco, opções de recuperação e uma manutenção contínua desses planos.

O objetivo do BCM é manter a capacidade de recuperação de serviços (neste caso das infraestruturas tecnológicas) de acordo com as necessidades, requisitos e prazos acordados do negócio. Inclui uma série de atividades para assegurar que os planos de continuidade e recuperação desenvolvidos bem como estratégias de políticas de continuidade, estão alinhados com a organização e com as prioridades do negócio.

Quando as organizações que operam internacionalmente começaram a exigir um único padrão internacional de segurança societal, foi desenvolvido o ISO 22301 - *Societal*

security -- Business continuity management systems --- Requirements. Este novo *standard* é o resultado de uma iniciativa global de interesse, cooperação e *inputs* sobre a necessidade de continuidade, contingência e recuperação das organizações na era da Globalização. Descreve uma *framework* que tem como objetivo melhorar a identificação de potenciais ameaças, avaliar o seu impacto e desenvolver a capacidade minimizar essa interrupção.

O ISO 22301 representa uma nova tendência mais abrangente de sistemas de gestão de continuidade de negócio que o ISO 27031, que é mais direcionada para "prontidão" das tecnologias.

De acordo com o inquérito de certificações da ISO.org, é possível verificar uma incursão tímida no ano de 2014, visto que a ISO 22301 foi desenvolvida em 2012 e não há registos de certificações/implementações em 2013. No topo da lista encontra-se a India, com perto de 30% de certificações, seguida pelo Reino Unido e Japão, conforme ilustrado pela figura 7.

Figura 7 – Distribuição de Certificações ISO 22301 em 2014
(ISO, 2014)

No mundo incerto de hoje e as preocupações crescentes com a continuidade de negócio e gestão de risco, prevê-se que o BCM e a respetiva certificação têm um mercado potencial de utilizadores.

Portugal conta apenas com 3 certificações em 2014, das 593 emitidas na Europa (37 países inquiridos). Além do Reino Unido (345), Holanda (64), Turquia (39), Grécia (29), Espanha (28), Roménia (21) e Polónia (20) apresentam o maior número de

certificações na Europa. Os restantes têm uma expressão mínima (12 países) como Portugal e muitos sem qualquer certificação (18 países).

A necessidade de um sistema de gestão de continuidade de negócio tem crescido rapidamente, impulsionando tanto o regulador de requisitos de conformidade como as organizações interessadas. Esses requisitos para continuidade sugerem que as organizações revejam os planos e resultados de testes do seu processo operacional, com o objetivo de minimizar as interrupções no negócio, mantendo a confiança na organização. A gestão de topo deve incorporar de forma proactiva a gestão da continuidade no modelo de negócio de forma a mitigar o risco de interrupções. Devido ao ritmo acelerado e volátil do mercado de hoje em dia, as organizações não podem correr o risco de terem planos desatualizados, incompletos ou ineficientes.

Além de identificar e gerir as ameaças atuais e futuras do negócio, o BCM mantém os processos de negócio críticos em funcionamento, minimiza o tempo de inatividade durante os incidentes, melhora o tempo de recuperação, e demonstra resiliência aos clientes, fornecedores e parceiros. É um processo contínuo com vários elementos (planos) diferentes, mas complementares: plano de mitigação de risco, plano de contingência, auditoria, plano de continuidade de negócio e plano de recuperação de desastres, entre outros.

No âmbito deste trabalho, o interesse recai sobre o BCP como já tem sido referido. Como consequência de elaboração de um plano de continuidade, poderá ser elaborado e implementado um DRP para as infraestruturas tecnológicas. Ou seja, o DRP não é um elemento do BCM, mas sim um tipo de plano de continuidade.

O custo de um BCP nunca pode ser exagerado, pois este plano é um dos pilares do BCM. A organização deve desenvolver um plano abrangente com base na sua dimensão e complexidade, com o objetivo de minimizar as perdas e as interrupções, e mitigar os efeitos negativos no negócio. O BCP define as etapas necessárias para a recuperação dos processos de negócio após um desastre, identificando a causa e a forma de comunicação com os elementos responsáveis pela recuperação dos serviços.

No caso de uma recuperação (total ou parcial) da infraestrutura, é necessário contemplar um DRP. Tal como todos os sistemas de gestão (segurança, continuidade, risco, etc.), o DRP também tem normas de boas práticas que podem ajudar a desenvolver um plano eficiente de recuperação: ISO 24762 - *Information technology -- Security*

techniques -- Guidelines for information and communications technology disaster recovery services.

O ISO 24762 fornece orientações sobre a recuperação das TIC como parte do BCM, aplicável tanto à organização como aos seus prestadores de serviços. Este *standard* especifica os requisitos para a implementação, operação, monitorização e manutenção de serviços de recuperação de TIC e respetivas instalações físicas; requisitos e práticas que os fornecedores de serviços TIC de uma organização devem seguir; orientação para a seleção de um local de recuperação alternativo; e orientações de melhoria contínua do DRP.

A recuperação constitui um dos aspetos mais importantes do BCP, pois a eficiência de uma organização depende do plano de recuperação e continuidade para restaurar as funções críticas de negócio num tempo aceitável. No entanto, a recuperação pode incluir procedimentos manuais! Seja qual for o modo de recuperação, a organização precisa de olhar para vários aspetos como o custo, tempo de interrupção permitido e aceitável, e executado de uma forma segura e rápida.

Terrorismo, desastres naturais, falhas de energia e outros riscos foram tidos em consideração para a integração do BCM e de planos de continuidade na gestão da organização. No entanto, continua a ser uma tarefa difícil, não só pelos custos associados e pela falta de "cultura organizacional", mas pela dificuldade de simular cenários de desastre. É por estas razões que muitas organizações não têm planos, estão obsoletos ou são inadequados.

2.5. Metodologia de sistemas BCM

A metodologia aplicada para a elaboração e desenvolvimento de planos de continuidade de negócios baseia-se nos modelos sugeridos pelas autoridades competentes de acordo com as práticas mais avançadas do mercado nesta matéria.

A globalização cresce a um ritmo acelerado e volátil pelo que as organizações não podem correr o risco de terem planos desatualizados, incompletos ou ineficientes. Procuram assim automatizar os processos de desenvolvimento de planos de continuidade e recuperação, atendendo às necessidades específicas do negócio e requisitos regulamentares.

O BCP deve identificar as ações que as organizações devem tomar para minimizar os efeitos adversos de eventuais potenciais desastres. O BCP deve incluir um programa preventivo, que suporte a estratégia desse plano, uma metodologia adequada, e um programa de revisão e manutenção. As organizações devem implementar uma metodologia faseada, de modo a analisar as áreas potenciais de vulnerabilidade, definir estratégias viáveis e implementar um BCP adequado aos processos de negócio.

Tal como muitos outros *standards*, o ISO 22301 aplica a metodologia PDCA para planear, implementar, monitorizar, manter, rever e melhorar a eficácia de um sistema de gestão de continuidade de negócio e respetivos planos, conforme a figura 8. Assim, garante-se a consistência com outros *standards* de sistemas de gestão, tais como a ISO 9001 – *Quality management systems*, ISO 14001 - *Environmental management systems*, ISO 20001 – *Information technology – Service management* e, obviamente, a ISO 27001.

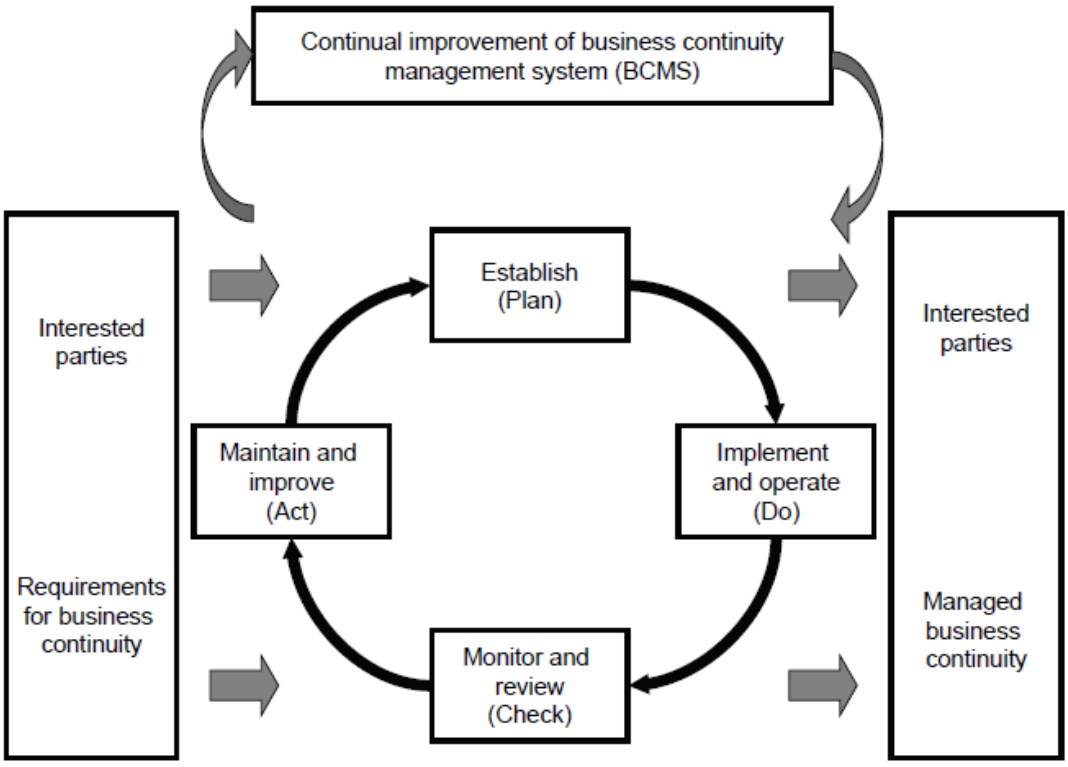


Figura 8 – Metodologia PDCA aplicada ao BCM
Fonte: **(ISO 22301:2012)**

A ISO 22301 é composta por 10 cláusulas: 0 - introdução, 1 – âmbito do *standard*, 2 – referências a normativos, 3 – termos e definições, 4 ao 10 - os requisitos de um sistema de gestão de continuidade de negócio. São estas últimas cláusulas que constituem a

metodologia PDCA, que por sua vez determinam a elaboração de um BCP. (ISO 22301:2012)

O componente *Plan* (P), cobre as cláusulas 4 a 7 e tem como objetivo estabelecer/planear a política de continuidade, objetivos, controlos, processos e procedimentos relevantes à melhoria da continuidade de negócio, de modo a garantir resultados devidamente alinhados com as políticas e objetivos definidos pela organização. A cláusula 4 introduz os requisitos necessários para definir o contexto e o âmbito do sistema BCM da organização. A cláusula 5 é um sumário dos requisitos específicos da gestão de topo e como esta articula com as expectativas da organização. A cláusula 6 descreve os requisitos relativos aos objetivos estratégico e princípios de um sistema BCM. O seu conteúdo estabelece oportunidades de tratamento de riscos decorrentes da avaliação de risco, bem como uma análise de impacto no negócio conhecido por *Business Impact Analysis* (BIA). A cláusula 7 suporta toda a execução do sistema BCM, enquanto documenta, controla, mantém e guarda informação tida como necessária.

O componente *Do* (D) tem como objetivo implementar e executar a política de continuidade de negócio, os controlos, processos e procedimentos definidos no componente anterior. Cobre a cláusula 8, que define os requisitos da continuidade de negócio, como lidar e desenvolver procedimentos para gerir um incidente disruptivo.

O componente *Check* (C), monitoriza e revê a *performance* da política de continuidade, reporta os resultados e determina e autoriza as ações necessárias para a remediação e melhoria da política. Assente na cláusula 9, define os requisitos para medir a *performance* do sistema BCM, a *compliance* com este *standard* e as expectativas da organização.

Por fim, o componente *Act* (A), mantém e melhora o sistema BCM através de medidas corretivas baseadas na avaliação e ajuste do âmbito, políticas e objetivos do negócio. A cláusula 10 do ISO 22301, identifica e age corretivamente sobre as não conformidades do sistema BCM.

Após explicação detalhada do ISO 22301, que define os requisitos de um sistema BCM, é possível desenvolver uma metodologia de elaboração de um BCP adequada ao negócio, juntamente com o desenvolvimento de uma consciência e sensibilização organizacional sobre a gestão da continuidade, risco e segurança da informação em todos os processos de gestão da organização.

3. Caracterização da Organização

A organização pública em estudo é a Agência para a Modernização Administrativa, Instituto Público (AMA, I.P.), que prossegue as atribuições da Presidência do Conselho de Ministros nas áreas da modernização e simplificação administrativa e da administração eletrónica, sob superintendência e tutela do Secretário de Estado da Modernização Administrativa, com sede em Lisboa (AMA, 2016a).

3.1. Missão e Visão

Tem por missão identificar, desenvolver e avaliar programas, projetos e ações de modernização e de simplificação administrativa e regulatória e promover, coordenar, gerir e avaliar o sistema de distribuição de serviços públicos, no quadro das políticas definidas pelo Governo.

Tem como visão a melhoria contínua na modernização na prestação de serviços públicos e de racionalização da despesa pública. Visiona igualmente ser um parceiro transversal a todos os órgãos internos e organismos da Administração Pública, capaz de disponibilizar soluções adequadas aos desafios colocados (AMA, 2014).

3.2. Orientações Estratégicas

A estratégia da AMA reflete as grandes linhas de orientação expressas nas Grandes Opções do Plano 2009-2013, no Programa do XVIII Governo Constitucional e do PGETIC[15], que situa a modernização administrativa entre as sete linhas fundamentais de modernização estrutural do país (AMA, 2014).

Toda a atividade da AMA visa construir mecanismos de interligação de procura e oferta de serviços públicos, concretizada através das TIC e da partilha do conhecimento. Deste modo, são definidos os seguintes objetivos estratégicos:

- Melhorar a qualidade da distribuição de serviços públicos
- Definir e implementar infraestruturas tecnológicas de apoio à modernização administrativa
- Simplificar o relacionamento entre a administração e os seus utentes

[15] Plano Global Estratégico para a Racionalização e Redução de Custos com as TIC, na Administração Pública, aprovado por Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro. https://tic.gov.pt/pgetic

- Avaliar os programas de simplificação e a qualidade dos serviços públicos
- Reforçar a eficácia, qualidade e eficiência interna

3.3. Modelo de Negócio

As políticas são direcionadas à excelência de serviço prestado aos utentes inerentes e ditam o comportamento dos processos de negócio (AMA, 2016b). De forma geral, são:

- Contribuir para a definição das linhas estratégicas e das políticas gerais relacionadas com a administração eletrónica, a simplificação administrativa e a distribuição de serviços públicos, incluindo a interoperabilidade na Administração Pública;
- Gerir e desenvolver redes de lojas para os cidadãos e para as empresas, em sistema de balcões multisserviços, integrados e especializados, articulando com os sistemas de atendimento em voz e rede;
- Promover a modernização da prestação e distribuição de serviços públicos orientados para a satisfação das necessidades dos cidadãos e das empresas;
- Promover as políticas de natureza central, regional e local na área da sociedade de informação, através da gestão dos espaços de Internet e outros semelhantes por si administrados, consultando as demais entidades com atribuições na sociedade de informação, sempre que tal se justificar;
- Apoiar a elaboração e implementação de plataformas e soluções de *e-learning*;
- Assegurar a representação externa e estabelecer relações de cooperação no âmbito das suas atribuições com outras entidades estrangeiras, nomeadamente no quadro na União Europeia e dos países de língua oficial portuguesa;
- Dar parecer prévio e acompanhar os projetos em matéria de investimento público e dar parecer prévio sobre a afetação de fundos europeus, no contexto da modernização e simplificação administrativa e administração eletrónica;
- Dinamizar e coordenar a rede interministerial de agentes de modernização e de simplificação administrativa;

- Promover a realização de estudos, análises estatísticas e prospetivas e estimular atividades de investigação, de desenvolvimento tecnológico e de divulgação de boas práticas, nas áreas da simplificação administrativa e regulatória e da administração eletrónica;
- Propor a criação e dirigir equipas de projeto, de natureza transitória e interministerial ou interdepartamental, para concretização, desenvolvimento e avaliação de ações de modernização e da simplificação administrativa e regulatória, designadamente através de avaliação de encargos administrativos da legislação, na vertente da sua simplificação corretiva.

3.4. Caracterização dos SI/TIC

A AMA foi criada em 2007 e resultou da extinção, por fusão, de vários organismos. Este processo de expansão, bem como as demais responsabilidades atribuídas em matéria de administração eletrónica e simplificação, exigiram uma gestão muito criteriosa dos recursos e o desenvolvimento de melhores instrumentos de gestão.

Em regime de *housing*, tem atualmente 99% da infraestrutura tecnológica virtualizada em equipamentos redundantes localizados no mesmo *datacenter*[16]. Com gestão remota e com um sistema de monitorização avançado, consegue garantir SLA's[17] de 99,99% de operacionalidade.

O sistema de *backup* tem uma taxa de sucesso de 95% e garante uma retenção de 30 dias e *restores*[18] granulares. Este sistema é partilhado com a entidade responsável do *datacenter* e o cofre das *tapes*[19] localizado no mesmo local.

Encontra-se atualmente a inventariar todos os serviços, relações e dependências, o que permite validar o impacto entre máquinas e serviços. É posteriormente exportada para uma ferramenta de arquitetura empresarial que permite mapear as várias camadas (tecnológica, aplicacional, processos e negócio), visualizar a evolução temporal das TIC, desenhar e otimizar soluções tecnológicas, bem como ter uma cartografia tecnológica da

[16] Local físico onde se encontram os SI/TIC.

[17] *Service Level Agreement*, consiste num acordo de níveis de serviço entre cliente/utilizador e fornecedor, definido pelo tipo de serviço, metas (temporais) e responsabilidades assumidas entre os intervenientes.

[18] Restauro das cópias de segurança.

[19] Dispositivo de armazenamento amovível utilizado nas cópias de segurança.

organização. Ao mapear as várias camadas, permite determinar a relação entre infraestruturas tecnológicas, serviços, processos e pessoas, bem como o impacto de qualquer alteração na arquitetura.

A AMA conta com uma equipa de Segurança, responsável pelo tratamento das ameaças às comunicações de voz e dados, coordenada com a equipa de Infraestruturas Tecnológicas, responsável pelo tratamento das vulnerabilidades dos sistemas e pelas falhas dos equipamentos físicos que suportam toda a infraestrutura virtual.

Ambas as equipas constataram a pertinência da existência de um plano de continuidade que permitisse recuperar a infraestrutura tecnológica no caso de um evento disruptivo. Esta necessidade foi transmitida à gestão de topo e, devido também a outros fatores, foi iniciado o desenvolvimento de um BCP suportado pelas diretrizes apropriadas identificadas no capítulo 2.

O capítulo seguinte caracteriza exatamente o problema e os fatores mais relevantes para a necessidade da existência de um plano de continuidade e recuperação.

4. Caracterização do Problema

Pretende-se neste capítulo caracterizar o problema que determinou a necessidade de elaboração de um BCP na organização em estudo.

A natureza dos serviços prestados e dos dados que têm sob sua guarda, confere a esta organização uma preocupação acrescida no que respeita à Continuidade de Negócio. Após a caracterização da organização e dos SI/TIC que a suportam, é percetível a necessidade da existência de um BCP, como em qualquer negócio atualmente. A organização em estudo depende muito da tecnologia bem como o seu modelo de negócio assenta totalmente nos SI. Assim, na ocorrência de uma disrupção é necessário assegurar o mínimo impacto na disponibilização desses serviços.

Mas como surgiu a necessidade e a sensibilidade para desenvolver um plano de continuidade na AMA?

Com vista a dar cumprimento à recomendação do Conselho de Prevenção da Corrupção (de 1 de julho de 2009), o Conselho Diretivo (CD) da AMA aprovou a 31 de março de 2010 o Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PGPRIC). O relatório anual de execução do plano relativo a 2013 (aprovado por despacho a 30 de junho de 2014), culminou no seguinte:

"Reformular ou elaborar um Plano mais consistente com a realidade orgânica e atribucional da AMA, que permita a adoção de mecanismos que garantam uma maior certeza e envolvimento de toda a AMA no seu cumprimento e melhoria, nomeadamente, a elaboração de relatórios parciais anuais pelos responsáveis pela implementação da medidas, com um conteúdo pré-definido mínimo que permita aferir o grau de execução, os intervenientes na execução, os custos de execução e implementação, os mecanismos da sua implementação e os meios de verificação de execução/indicadores de efetividades, os riscos e, quando for caso disso, os constrangimentos que levaram à não implementação de medidas.

Que o Plano a adotar preveja mecanismos de controlo e uma monitorização mais eficiente, nomeadamente com a elaboração de quadros periódicos de monitorização/acompanhamento, designadamente trimestrais." (AMA, 2015)

Durante o levantamento de informação, avaliação de risco e impacto no negócio, foram identificados os processos suscetíveis de geração de riscos, elencadas as situações de risco e a sua responsabilidade face à organização da AMA, das quais destacam-se:

PROCESSOS, RISCOS E RESPONSABILIDADES					
PROCESSO		SITUAÇÕES DE RISCO	PO	GR	RE
Infraestruturas Tecnológicas	Gestão de identidades e perfis de acesso	Acesso interno não autorizado a informação reservada	Fraco	Médio	Elevado
	Continuidade de negócio	Inexistência de plano de recuperação da informação e das operações em caso de desastre	Elevado	Elevado	Elevado
	Cibersegurança	Intrusões explorando vulnerabilidades dos sites que ponham em causa a disponibilidade dos mesmos ou a confidencialidade/integridade da informação	Elevado	Elevado	Elevado

Legenda - PO: Probabilidade de ocorrência; GR: Gravidade; RE: Reversibilidade dos efeitos.

Tabela 1 – Processos suscetíveis de geração de riscos na AMA
Adaptado de (AMA, 2015)

Pela primeira vez constata-se a necessidade de um processo de continuidade de negócio. As medidas de prevenção e de controlo interno dos riscos foram determinadas em função dos processos identificados na avaliação de risco, a qual deu lugar à execução da medida: implementação de um *Disaster Recovery* e *Business Continuity* para os sistemas críticas da AMA, durante o segundo semestre de 2016.

A AMA, responsável pela elaboração do PGETIC e por garantir o funcionamento contínuo dos sistemas transversais à Administração Pública, sente uma obrigação acrescida de melhorar a eficiência dos processos internos e melhorar a qualidade dos serviços prestado.

De acordo com o portal tic.gov.pt[20] é possível verificar o estado de execução das medidas do PGETIC e, à data de elaboração deste documento, apenas o Ministério da Solidariedade, Emprego e Segurança Social apresenta uma taxa de execução de 65% de um BCP para todo o ministério e organismos respetivos. Não há registos de planeamento e implementação de um BCP noutros ministérios ou institutos.

A AMA reconhece a resiliência à generalidade de alguns riscos, mas não ao desastre total do *datacenter* ou parcial (em caso de falha das comunicações de dados). Apesar da redundância de infraestrutura tecnológica e de comunicações, da segurança da

[20] https://tic.gov.pt – portal das tecnologias da informação da Administração Pública.

informação (tanto dos sistemas como de acesso ao *datacenter* e outros controlos), encontra-se tudo no mesmo local físico. Em caso de um evento disruptivo, não é possível dar continuidade ao negócio nem recuperar num tempo aceitável e, eventualmente, associado a uma perda significativa de dados. Todos os serviços disponibilizados e transversais seriam afetados, colocando em causa não só o negócio da AMA, mas de também de todos os organismos públicos, parceiros e clientes.

Além dos sistemas transversais, a AMA é responsável pela racionalização dos *datacenters* e unificação das comunicações de dados e voz da PCM, pelo que acresce também a responsabilidade de garantir a continuidade e operacionalidade destas funções. No entanto, tem havido alguma resistência na migração dos restantes institutos públicos da PCM, mas que com um plano de continuidade e recuperação das TIC da AMA seria um incentivo ao cumprimento de várias medidas do PGETIC. Ou seja, haveria alguma confiança nos organismos e nos parceiros em utilizar os serviços prestados pela AMA, bem como na cedência/transferência das funções informática.

A sensibilização e a consciência das equipas de negócio, nomeadamente das equipas da Direção de Sistemas de Informação da AMA, para a continuidade e recuperação do negócio, gestão do risco e segurança da informação, aliadas a estas obrigações legais, diretivas e problemática internacional, foram os fatores decisivos para arrancar com o projeto de um BCP.

Aliada a isto, prende-se igualmente com a necessidade de recuperar a infraestrutura tecnológica num tempo considerado aceitável. Apesar de se encontrar em *housing*, havendo de alguma forma transferência da responsabilidade pela segurança física das instalações e controlo de acessos, é necessário garantir a recuperação do *datacenter*, dos sistemas e dados respetivos em caso de desastre.

Esta problemática da necessidade de continuidade de negócio e recuperação é sentida em todas as organizações atualmente. Vivem-se tempos de instabilidade e insegurança, causados por fatores socioeconómicos, ambientais, tecnológicos, entre outros, que colocam em causa a organização e tudo o que depende dela. Desafios à sustentabilidade das organizações podem fechar empresas, perder informação vital, levar à carência económica, e tantos outros exemplos, pelo que a sua continuidade deve ser garantida através de sistemas e planos adequados e bem estruturados para minimizar o impacto na vida das Pessoas.

5. Apresentação do Estudo de Caso

Foi desenvolvido um estudo de caso na organização pública identificada e caracterizada no capítulo 3, de forma a validar a metodologia de desenvolvimento de um BCP. Este capítulo é um registo de trabalho para a especificação, planeamento e operacionalização de um BCP, com focos na recuperação dos serviços IT do *datacenter* dessa organização e tem como fonte o plano de continuidade e recuperação realizado pela equipa de projeto da AMA (AMA, 2016c).

O *datacenter* da AMA disponibiliza um conjunto de serviços para o exterior. Na ocorrência de um desastre é necessário assegurar o mínimo de impacto na disponibilização desses serviços. A iniciativa em causa propõe-se a estabelecer um plano de recuperação dos serviços de IT na ocorrência de um desastre, identificar e operacionalizar as condições necessárias para a execução do plano.

5.1. Metodologia de elaboração do BCP

Baseada na ISO 22301:2012, nomeadamente no ciclo PDCA, foi desenvolvida uma metodologia para a elaboração do BCP da AMA. A metodologia desenvolvida é constituída por 7 etapas que perfazem um ciclo da iniciativa conforme demonstrada na figura 9.

Figura 9 – Metodologia de elaboração do BCP

O primeiro ciclo de etapas estabelece as fundações e práticas necessárias para a especificação, planeamento e operacionalização de um plano de continuidade. Os ciclos seguintes são de melhoria contínua para assegurar que o plano se mantém atual e adequado às necessidades da organização.

A primeira e segunda etapa, têm como objetivo global avaliar o esforço de um BCP, validando o âmbito e detalhe do plano de continuidade, tendo em conta um inventário dos processos ou unidades de negócio necessários, identificando os intervenientes e metodologia do projeto. Não define custos, linha temporal ou recursos necessários à sua elaboração. Já o levantamento de informação consiste em conhecer o negócio e toda a infraestrutura tecnológica que a suporta. Contempla igualmente as atividades de identificação dos artefactos, pessoas e procedimentos envolvidos no plano de continuidade e na definição dos repositórios para essa informação.

A BIA é o passo seguinte na elaboração de um BCP. A terceira etapa identifica as ameaças, enquadra a avaliação de risco e determina o impacto no negócio. Existe um número de ameaças que podem ocorrer a qualquer momento e afetar os processos de negócio de uma organização. Cada evento deve ser analisado de modo a identificar-se as medidas de redução, níveis de interrupção e respetivo impacto. Nesta fase também tem o objetivo de definir tempos de comunicação e recuperação dos processos de negócio críticos, identificar os requisitos e as melhores práticas a serem seguidas, determinar o tempo e esforço de execução de um plano.

Com base nas etapas anteriores, é criado o BCP. A etapa 4, estratégia de recuperação e continuidade, identifica os procedimentos e políticas do plano de continuidade. Por sua vez, este inclui planos de recuperação a um nível granular e/ou externos (fornecedores e parceiros), que especificam respostas a situações de emergência.

A fase do planeamento consiste na definição dos pontos omissos da primeira etapa: tudo que tenha relevância para a operacionalização do plano. Esta é acompanhada pela sexta etapa, a execução do plano. No sentido de avaliar a viabilidade do plano, devem-se realizar testes funcionais de modo a verificar se todos os processos de negócio críticos funcionam como esperado.

Como indicado, um BCP nunca está completo, iniciando novo ciclo. Quantos mais detalhados forem os procedimentos de controlo, mais eficiente e eficaz será o plano. O plano deve ser melhorado, decorrendo das atividades de teste e monitorização após a sua

implementação, devendo incluir um planeamento calendarizado de auditoria e revisão. Um dos objetivos da auditoria é exatamente a melhoria contínua dos controlos e procedimentos de recuperação e continuidade do negócio.

O tempo de recuperação é dos componentes do plano mais importantes para o negócio e que determina em certa parte a sua eficiência, continuidade e recuperação. Se o tempo de recuperação for demasiado alto, pode colocar em causa os processos de negócio mais críticos para a organização, perder dados e clientes, e colocar em risco parceiros e fornecedores.

Elementos como o *Recovery Point Objective* (RPO) – determina o tempo máximo aceitável de perda de dados, *Recovery Time Objective* (RTO) – determina o tempo máximo aceitável para ativar todos os sistemas críticos, *Work Recovery Time* (WRT) – determina o tempo máxima aceitável para verificar os sistemas e a integridade dos dados e *Maximum Tolerable Downtime* (MTD) – determina o tempo máximo de uma disrupção sem consequências para o negócio, são constantemente avaliados e ajustados no plano de acordo com as alterações mais recentes da organização e respetivas necessidades. Para melhor perceção destes elementos, a figura 10 representa a linha temporal para recuperação de um processo em caso de disrupção.

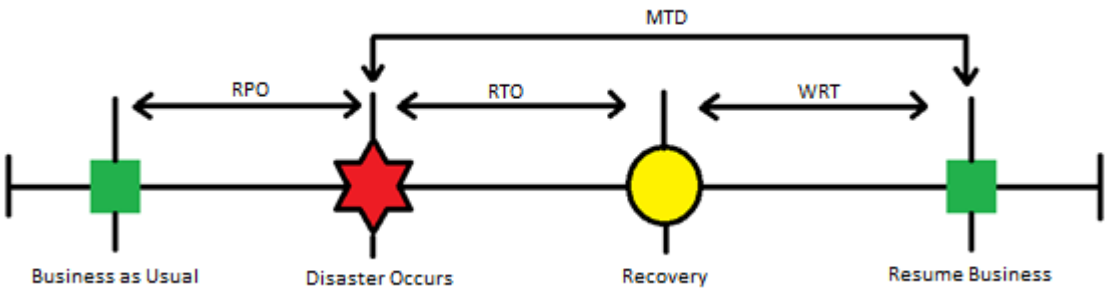


Figura 10 – Linha temporal de recuperação
(Aggarwal, 2015)

De acordo com a metodologia definida para a elaboração do BCP da AMA, cada etapa foi decomposta na estrutura de trabalho seguinte:

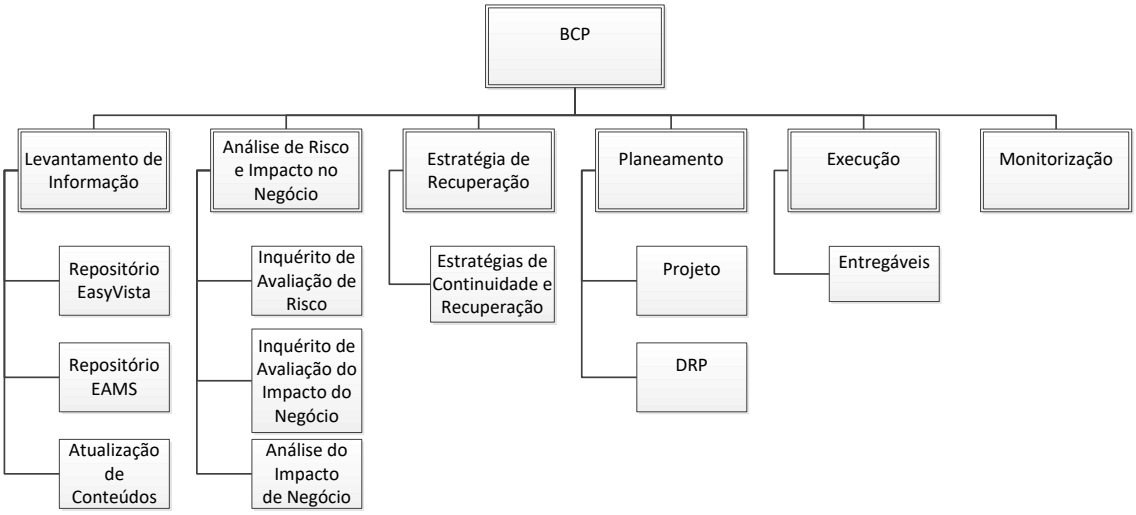


Figura 11 – *Work Breakdown Structure*
(AMA, 2016c)

Cada subcapítulo seguinte representa uma etapa, como parte integrante do BCP, elaborado pela equipa de projeto da organização em estudo.

5.2. Levantamento da Informação

Esta etapa contempla as atividades de identificação dos artefactos, pessoas e procedimentos envolvidos no BCP e na definição dos repositórios dessa informação, onde é detalhado o modelo de dados dos repositórios, processo de sincronização entre os repositórios, responsáveis, perfis de utilizadores, como aceder às ferramentas e criação e edição de informação no sistema de arquitetura empresarial.

Durante o processo de identificação e levantamento da informação, são definidas as responsabilidades de cada uma das peças envolvidas na solução de continuidade e recuperação.

5.2.1. Processos de identificação e levantamento da informação

A informação dos artefactos foi identificada e caraterizada em sessões de trabalho da equipa de projeto e em trabalho individual estipulado durante as sessões de trabalho.

Na primeira fase foram recuperados documentos Excel e documentos de exportação de ferramentas operacionais que foram consolidados num único documento de Excel, posteriormente importado para o repositório do *EasyVista*[21].

Tendo em consideração a natureza da utilização do *EasyVista*, que é uma ferramenta de *Service Management* e como tal tem um nível limitado de detalhe dos artefactos, foi considerada também a ferramenta EAMS (*Enterprise Architecture Management System*)[22] para suportar um modelo de dados mais detalhado e permitir a realização de análise mais complexas.

Os tipos de artefactos considerados nesta foram os seguintes:

- Serviços
- Aplicações – que fornecem os serviços
- Bases de Dados – que suportam as aplicações
- Servidor Aplicacional – que aloja as aplicações
- Servidor de Base de Dados – que aloja as bases de dados das aplicações
- Servidor Web – que aloja e/ou disponibilizam as aplicações
- Servidor DNS – que publicam as aplicações e serviços

5.2.2. Operacionalização da solução

Este ponto contempla as atividades de operacionalização da solução bem como os procedimentos que asseguram a manutenção e atualização da informação referente aos artefactos envolvidos no plano de continuidade e recuperação.

A ferramenta *EasyVista* suporta as atividades de apoio ao utilizador da AMA e mantém o inventário dos artefactos necessários para essa operação. Foram estabelecidos os seguintes princípios da solução:

- A informação do repositório *EasyVista* é *master*;
- A informação do *EasyVista* é a suficiente para as atividades de apoio ao utilizador

No entanto, esta informação não é suficiente para análise complexas e caracterização detalhada da Arquitetura Aplicacional e de Infraestrutura da AMA.

[21] É uma ferramenta de gestão de tickets e que fornece ferramentas como uma base de dados de gestão de mudança (CMDB). URL: http://www.easyvista.com/pt/

[22] É uma ferramenta de arquitetura empresarial. URL: http://www.linkconsulting.com/eams/

A ferramenta EAMS serve de repositório e instrumento de análise dos dados mais detalhados. A informação dos artefactos no *EasyVista* é considerada *master*, mas muito menos detalhada. O repositório EAMS mantém toda a arquitetura dos artefactos e gere de forma independente detalhes que não são persistidos no *EasyVista*. Esta abordagem permite realizar análise de impacto com maior detalhe e caracterizar com mais detalhe as transformações nos vários tipos de Arquitetura Empresarial da AMA.

O processo de atualização da informação da solução resume-se ao processo representado na figura 12.

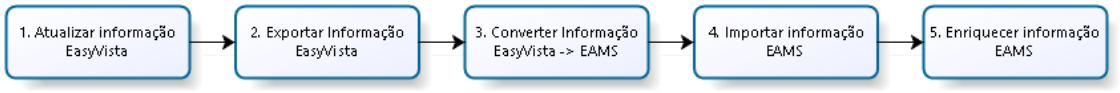


Figura 12 – Processo de atualização da informação
(AMA, 2016c)

1. Atualizar informação *EasyVista*, consiste na manutenção da informação na CMDB.
2. Exportar informação *EasyVista*, corresponde à ação de aceder aos relatórios de exportação da informação, compostos por dois ficheiros CSV: o primeiro tem informação sobre todos os itens de configuração que estão presentes no repositório e o segundo tem a informação sobre as relações entre todos os itens de configuração. Estes ficheiros vão servir de *input* à tarefa seguinte que irá consistir na conversão dos dados de modo a serem importados para o repositório do EAMS.
3. Converter informação *EasyVista* -> EAMS, consiste na conversão dos dados exportados para uma meta-dado passível de importação pelo EAMS, de forma automática.
4. Importar informação EAMS, permite carregar a informação convertida anteriormente no repositório arquitetural do EAMS
5. Enriquecer informação EAMS, é o enriquecimento da informação que já se encontra no repositório. Permite completar as relações entre as várias camadas (tecnológicas, aplicacionais, processuais e pessoas), sendo possível mapear e desenhar todas as suas relações e dependências.

5.3. Avaliação de Risco e Impacto no Negócio

Este subcapítulo constitui um registo das atividades e principais resultados obtidos no âmbito da Avaliação de Risco e Análise de Impacto no Negócio, enquadrado na especificação, planeamento e operacionalização do plano de continuidade e recuperação dos serviços IT do *datacenter* da AMA.

A análise de riscos e análise para o negócio constantes neste plano resultam na definição de requisitos para a implementação futura do DRP. Pelo que, os resultados apresentados são *inputs* importantes para as atividades de definição de Estratégias de Recuperação e Continuidade e do DRP.

5.3.1. Avaliação de Risco

Existem várias ameaças que podem ocorrer a qualquer momento e afetar os processos de negócio ou serviços vitais da AMA. A concretização destas ameaças poderá resultar em incidentes que possam comprometer a normal operação dos SI e consequentemente afetar os processos de negócio ou serviços deles dependentes. Alguns destes incidentes, pela sua severidade, poderão ter um impacto considerável, resultando em situações de emergência ou desastre.

O processo de Avaliação de Riscos deve ainda conduzir a atividades que, analisando os riscos de maior severidade, conduzam à identificação de medidas de mitigação do risco, reduzindo a probabilidade e/ou impacto desse risco se concretizar. Na sequência desta avaliação, será também efetuada, para os serviços mais críticos, a Análise de Impacto para o Negócio, que considerando os requisitos de serviço esperados e exigidos irá resultar na concretização deste plano e respetivo DRP.

O risco associado a estas situações é calculado considerando a probabilidade de concretização e o seu impacto potencial:

$$\text{Risco} = \text{Probabilidade} * \text{Impacto}$$

O valor desse risco indicará a severidade do mesmo, tendo sido definido os níveis de risco de acordo com a tabela seguinte, com base na matriz de avaliação de risco sugerida pelo anexo E do ISO 27005. Quanto maior o valor, maior o risco. Representado graficamente de verde para vermelho (de menor para maior risco).

		Impacto					
		1	2	3	4	5	6
Probabilidade	1	1	2	3	4	5	6
	2	2	4	6	8	10	12
	3	3	6	9	12	15	18
	4	4	8	12	16	20	24

Tabela 2 – Tabela de risco da AMA

Para as ameaças identificadas e caracterizadas é atribuída a respetiva probabilidade de ocorrência, de acordo com a tabela seguinte.

Probabilidade	Escala	Frequência
1	Muito pouco provável	1 vez de 4 em 4 anos
2	Pouco provável	1 vez de 2 em 2 anos
3	Provável	1 vez por ano
4	Muito provável	Várias vezes por ano

Tabela 3 – Caracterização da probabilidade de ocorrência de uma ameaça

O impacto a considerar pode ser tangível ou intangível. Quando é considerado tangível, deve-se definir intervalos de valores monetários que dimensionam a perda financeira. Cada intervalo tem um valor de pontuação associado. Regra geral, podem ser consideradas as seguintes categorias de impacto tangível:

Categoria	Descrição
Perda de Receitas	Perda de recursos provenientes de venda de bens ou serviços
Receitas extraordinárias	Temporárias de pessoal, horas extras, equipamentos, serviços
Legal e Jurídico	Multas, penalidades, problemas de conformidade, as obrigações contratuais, os passivos financeiros

Tabela 4 – Caracterização do impacto tangível

Face ao tipo de serviço prestado e quantidade de entidades envolvidas, que iriam requerer um maior número de recursos e tempo para a sua avaliação, foi considerado mais adequado e produtivo considerar apenas o impacto intangível. Estes não têm, por definição, um valor monetário quantificável. No entanto, se esse tipo de impacto medir a perturbação que a indisponibilidade ou mau funcionamento de um serviço pode causar, o seu nivelamento é mais fácil de quantificar pelos técnicos envolvidos na análise.

Assim, para avaliar o impacto intangível dos vários serviços identificados, foram definidos os seguintes níveis:

Impacto	Efeito
1	Não existente
2	Mínimo
3	Moderado
4	Moderato Alto
5	Alto
6	Severo

Tabela 5 – Caracterização do impacto intangível face à ocorrência de uma ameaça

O impacto é estabelecido com base em níveis de valor permitindo a comparação de criticidade entre os serviços. Quanto maior o nível, maior a criticidade.

Face a um conjunto de ameaças identificadas com base no ISO 27005, ficou definido em sessão de trabalho da equipa de projeto que o modelo de risco deve considerar as ameaças que configurem as situações mais críticas, resultando numa simplificação do modelo e permitindo uma análise mais profunda das soluções de continuidade de negócio, tendo em conta a missão e restrições temporais deste projeto.

Para a ameaça considerada – Desastre – foi considerada uma probabilidade de nível 1 (muito pouco provável). Valor que serviu de cálculo ao risco dos vários serviços analisados e que torna o valor do risco igual ao nível do impacto.

O levantamento de informação para a Avaliação de Risco foi através do preenchimento do inquérito de Avaliação de Risco, tendo em conta a ameaça genérica "Desastre". Para cada serviço de IT foi quantificada a probabilidade e impacto, que resulta no risco inerente a cada serviço.

De notar que a Gestão dos Riscos não deve limitar-se à avaliação efetuada no âmbito deste projeto, devendo encarar-se como um processo a interiorizar na AMA, de forma a permitir o seu acompanhamento. A dinâmica da organização e fatores externos, poderão elevar ou baixar o nível dos riscos. Para tal, estes devem ser monitorizados e documentados, aferindo a necessidade de aplicação de novas medidas de controlo em função das características e severidades desses riscos. A gestão de topo, neste caso o Conselho Diretivo, deve ser notificado das alterações importantes aos riscos como componente essencial ao processo de avaliação do BIA e respetiva tomada de decisões.

5.3.2. Análise de Impacto no Negócio

O propósito da BIA neste contexto é identificar e priorizar os serviços de IT e caracterizar o impacto da indisponibilidade dos serviços. Esta análise é constituída pelos seguintes passos:

1. Identificar serviços e respetiva criticidade – os serviços suportados pelos sistemas e o impacto da disrupção dos sistemas nos serviços é determinada com base no impacto de indisponibilidade e a estimativa tempo de indisponibilidade. O tempo de inatividade deve refletir o máximo que uma organização pode tolerar, mantendo a sua missão. Os requisitos de tempo de recuperação estão diretamente relacionados com a criticidade do impacto.
2. Identificar requisitos dos recursos. Identificação realista do esforço de recuperação necessário para se retomar as operações da forma mais rápida possível e financeiramente viável.

3. Identificação das prioridades de recuperação dos recursos. Com base nos resultados das atividades anteriores é possível estabelecer a relação entre recursos a alocar e a criticidade dos serviços. É possível estabelecer prioridades na sequenciação das atividades de recuperação.

A tarefa fundamental da BIA é compreender quais os processos mais críticos para o negócio e o impacto que a disrupção desses processos têm no negócio. Os processos de negócios que a AMA gere dependem dos serviços IT disponibilizados, pelo que a análise de impacto considerou na sua análise os serviços disponibilizados aos utentes.

O levantamento de informação para a BIA foi feito através da disponibilização de inquérito, em tabelas preparadas para o efeito exemplificada pela tabela 6. Neste inquérito, os serviços foram caracterizados e atribuindo-lhes os requisitos temporais para a recuperação dos mesmos.

Atributo	Descrição
Entidade	Identifica a Entidade da Administração Pública dona do serviço.
Tipo	Classifica o serviço como sendo de Negócio ou de Suporte.
Serviço	Nome do serviço
Descrição	Descrição do serviço
Crítico para o negócio	Classifica o serviço como sendo crítico ou não crítico para o negócio.
Dependência de outros serviços	Identifica outros serviços dos quais o serviço possa depender. Este atributo deve, quando possível, ser derivado de relacionamento efetivos, como comunicação entre aplicações, partilha de infraestrutura, etc.
Responsáveis	Identifica o responsável de negócio do serviço
Aplicações	Identifica as aplicações que suportam o serviço.
RTO - *Recovery Time Objective*	Determina a quantidade tolerável máxima de tempo para repor o serviço.
RPO - *Recovery Point Objective*	Período de tempo perdido aceitável. Quantidade de dados perdida aceitável.

Tabela 6 – Características e requisitos dos serviços

Estes inquéritos requereram a recolha de dados e análise pela equipa de projeto, que os devolveram preenchidos, com que informação que, depois de trabalhada, resultou num documento final.

No entanto, não foi possível complementar a informação com os dados dos responsáveis dos diferentes serviços e equipas de recuperação, por esses não terem sido preenchidos atempadamente ou por não serem fiéis à realidade (ou seja, o serviço desse responsável era sempre o mais crítico). Estes dados foram introduzidos no EAMS, para que seja possível a sua consulta de forma centralizada e apoiando a tomada de decisões futuras (além dos benefícios do mapeamento da arquitetura tecnológica da organização).

A informação disponibilizada contempla o impacto resultante do comprometimento dos serviços analisados. O facto de se considerar os serviços de IT em detrimento da análise dos processos de negócio, resulta que o impacto avaliado e apresentado na Avaliação de Risco terá um impacto equivalente ao nível do negócio, e que permitiu classificar estes serviços quanto à sua criticidade e impacto.

A análise aos dados de impacto no negócio e necessidades identificadas com a equipa de projeto, conduziu à definição de dois cenários, que requerem a ativação do DRP, para os quais está a ser definido o BCP.

O cenário de Desastre, com recuperação total, considera que o *datacenter* da AMA foi comprometido, ficando inacessível, sendo necessário retomar e recuperar os serviços de IT, a partir de um *site* alternativo. É assim necessário garantir a disponibilização dos recursos de processamento no *site* secundário, como também a replicação e/ou a recuperação dos dados entre os dois *datacenter*. Os requisitos de implementação de um *datacenter* secundário, resultam da caracterização feita ao nível da criticidade e consequentes RTO e RPO.

O outro cenário considerado que, não sendo de Desastre completo, comprometam as comunicações de dados e voz e que obrigue a ativar o DRP. A falha do operador ou dos equipamentos de rede podem originar essa situação. Este cenário diverge do anterior por possibilitar RPO's iguais a zero, sendo possível retomar os serviços sem perda de dados.

5.3.3. Conclusão da Análise de Impacto de Negócio

Como a probabilidade de um desastre é reduzida, a avaliação dos riscos resulta do impacto que o comprometimento dos vários serviços possa ter. Após analisado os dados recolhidos do catálogo de serviços, foram identificados os serviços com maior impacto (5 - Alto e 6 - Severo):

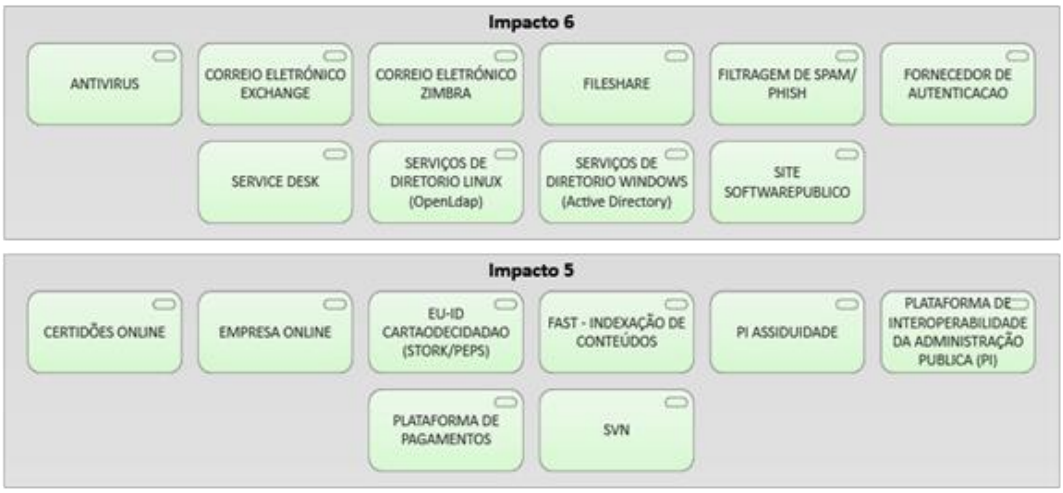


Figura 13 – Serviços com maior impacto

A análise de impacto permitiu igualmente identificar requisitos temporais dos diferentes serviços (no que respeita ao RTO), tendo sido definidos como de recuperação imediata:

Figura 14 – Serviços de recuperação imediata

No que respeita à quantidade aceitável de dados perdidos (RPO), o resultado do levantamento aponta para que os seguintes serviços não tivessem qualquer perda de informação:

Figura 15 – Serviços sem perda de informação

5.4. Estratégia de Recuperação

Este subcapítulo aborda a estratégia de recuperação dos serviços do *datacenter* (*site* principal) para o *datacenter* alternativo (*site* secundário*)*.

Nesta estratégia foi assumido o risco de não ter uma infraestrutura redundante no *second site*, considerando-se que este é um risco contido, pois só deverá ser considerado em caso de ativação do DRP e por um tempo que se espera reduzido. Caso a recuperação do *site* principal se prolongue por mais tempo que o esperado (1 mês) deverá ser avaliada pela equipa da AMA a necessidade de garantir a redundância do *site* secundário, adquirindo o respetivo equipamento. Não se trata de mudar a solução, mas adquirir equipamento complementar para os componentes críticos da infraestrutura.

Em alguns casos o investimento estimado poderá resultar numa renovação da infraestrutura principal, pois o equipamento a adquirir sendo mais recente e, por isso, com melhor desempenho poderá ser instalado no *site* principal, passando o atual equipamento para o *site* secundário.

A implementação de um *site* secundário para recuperação, pressupõe que, na generalidade das componentes, os serviços estejam replicados, mas não ativos.

Para garantir que, em caso de necessidade, os serviços se encontram devidamente configurados, bem como a celeridade das atividades de ativação do *site* secundário, torna-se crucial planear testes periódicos. Estes testes são igualmente abordados no DRP e não devem ser descurados.

Como procedimento normal de operação deverão ser definidas as atividades de monitorização que controlem se a replicação está a decorrer como esperado. Caso contrário, detetem atempadamente necessidades de correção aos procedimentos implementados.

Por não se enquadrar no âmbito deste trabalho, por conter uma especificidade técnica avançada e por questões de confidencialidade e segurança da organização em estudo, alguns pontos da estratégia de recuperação serão omitidos, nomeadamente as características da infraestrutura tecnológica e de comunicações existente e da respetiva solução de recuperação.

5.4.1. Identificação de requisitos técnicos dos serviços aplicacionais

Nesta fase da etapa são apresentadas as estratégias a adotar de forma a garantir a disponibilidade da infraestrutura, sistemas e dados no ambiente de recuperação.

Para além da identificação de necessidades ao nível dos servidores, são analisadas as estratégias para replicação e recuperação (*backup*/*restore*) de sistemas e dados.

A estratégia de replicação a adotar, foi uma das primeiras a ser analisada, uma vez que as várias opções poderiam condicionar a estratégia a selecionar para os outros componentes da infraestrutura, nomeadamente na componente de rede.

O *site* secundário deverá ter capacidade para alojar o ambiente de produção[23], não estando previsto que o mesmo seja montado em *cluster*[24], assumindo-se o risco de não ter redundância.

Este risco é controlado, pois tratando-se de um ambiente de recuperação que só será ativado em caso de falha do *site* principal, que por sua vez é redundante. Assim a probabilidade de os servidores do *site* secundário falharem simultaneamente que o *site* principal, é muito reduzida.

Em cenário de catástrofe, caso se venha a verificar que a paragem do *site* principal irá prolongar-se mais do que o desejado, deverá ser avaliada a necessidade de instalação, no *site* secundário, de servidores de *backup* à semelhança do ambiente existente no *site* principal.

Esta opção de implementação poderá não requerer a aquisição de novos equipamentos, pois, dependendo do cenário de desastre que vier a acontecer, poderá conseguir aproveitar-se equipamento do *site* principal e deslocado para o *site* secundário.

Em alternativa, visto que a replicação é garantida ao nível da plataforma de virtualização, pode ser adquirido equipamento de outro fabricante com uma capacidade de processamento semelhante e eventualmente a um custo inferior.

Optando-se por equipamento novo, poderá substituir os equipamentos atuais do *site* principal, deslocando-se os mais antigos para o *site* secundário. Esta operação, se programada e faseada, não acarreta paragem dos serviços.

[23] Regra geral, os ambientes de servidores aplicacionais são compostos por Produção, Testes/Qualidade e Desenvolvimento. Cada ambiente tem a sua função com objetivo de garantir a qualidade de desenvolvimento de *software*, de acordo com a ISO 25010:2011

[24] Um conjunto de servidores redundantes, interligados de forma a disponibilizarem um serviço. Melhora o serviço, disponibilidade e escalabilidade do sistema. Em caso de falha de um dos servidores, os restantes continuam a funcionar.

A adoção desta alternativa irá permitir conseguir algumas poupanças em termos de licenciamento da plataforma virtual que a suporta, como dotar o *datacenter* de uma nova infraestrutura e respetivo *assurance*[25].

A recuperação de desastres é um processo que pretende proteger os ativos que compõe a infraestrutura tecnológica na ocorrência de uma catástrofe ou falha que impeça o normal funcionamento dos serviços. A existência de um DRP permite a execução de um processo, automatizado, que simplifica e reduz os custos com a reposição dos serviços considerados críticos.

Os principais requisitos para a recuperação de desastres, adequados às necessidades da AMA:

- Replicação automatizada dos serviços a custo acessível
- Recuperação rápida com automatização
- Recuperação confiável
- Automatização de testes sem interrupção
- Testes simplificados dos planos de recuperação

Após o levantamento dos serviços críticos identificados na BIA da AMA, foi realizada uma análise da infraestrutura que lhes dá suporte e verificou-se que os servidores que suportam os serviços críticos estão, na sua maioria, suportados sob a plataforma de virtualização.

Esta plataforma de virtualização oferece uma solução de recuperação de desastres que fornece um mecanismo de proteção simples, confiável e económica para servidores virtualizados. Este mecanismo de recuperação permite a automação do processo de recuperação, a gestão centralizada dos planos de recuperação a aplicar e a execução de testes de recuperação não disruptivo dos sistemas produtivos. Uma vez que o processo é potenciado automatizando as tarefas de recuperação, é possível eliminar a complexidade e risco da execução de processos manuais, baixando também os tempos de RTO.

Permite igualmente implementar uma solução de replicação dos servidores virtuais agnóstica, no que diz respeito a soluções de *storage*[26], não ficando a AMA dependente do fabricante e dos seus mecanismos de replicação de dados. A replicação é

[25] Garantia, suporte e manutenção, neste caso dos servidores e sistemas licenciados.
[26] Equipamento de armazenamento de dados de grande capacidade.

efetuada ao nível do *hypervisor*[27] e aplicada aos servidores virtuais que suportam os serviços críticos. Esta solução tem ainda outras vantagens, tais como, a flexibilidade do RPO definido, que vai dos 15min às 24h, a possibilidade de criar múltiplos pontos de restauro e a eficiência de largura de banda, utilizando mecanismos de compressão que reduzem o tráfego gerado durante a replicação.

O ponto central do armazenamento da informação está numa *Storage Area Network* (SAN) e suporta toda a infraestrutura virtual.

Assim, para a implementação da solução, optou-se pela expansão da infraestrutura virtual da AMA, pela aquisição de um conjunto de servidores e uma nova SAN para suporte da infraestrutura virtual no *site* secundário.

Permite-se assim que a componente virtual da AMA fique dividida entre os dois *datacenters*, principal e secundário, mas com total sincronismo dos servidores que suportam os serviços críticos. Estas tecnologias permitem que toda a infraestrutura seja vista nas consolas de gestão de qualquer um dos *sites*, possibilitando a utilização e otimização dos recursos, e em caso de desastre recuperar os serviços a partir de qualquer um dos locais.

O *hypervisor* em questão permite a execução de testes automatizados dos planos de recuperação numa rede isolada, de modo a evitar o impacto nos servidores de produção.

Os testes de planos de recuperação podem ser executados tantas vezes quanto as vezes que forem necessárias, sem interrupção dos serviços em produção, para garantir a previsibilidade dos RTO e que a replicação ocorre dentro dos RPO definidos para cada um dos serviços.

O intervalo máximo entre testes de recuperação, não deve ser menor que a frequência de testes de recuperação de cada serviço crítico, com a consequência dos processos de recuperação sujeitos a ficarem desatualizados ou inadequados. O resultado da execução do procedimento para testes de recuperação, definido para cada serviço crítico identificado, devem ser registados de forma a garantirem uma base de melhoria contínua e manutenção dos planos.

Relativamente à solução de *backups*, a AMA utiliza um sistema partilhado com a entidade responsável pelo *datacenter* (conforme indicado anteriormente, encontra-se em

[27] Sistema de administração de plataformas de virtualização.

housing). Este recurso é igualmente um componente a ter grande consideração na estratégia de recuperação.

É desejável que o sistema de *backups* do *site* secundário seja semelhante, de forma a permitir que seja possível a recuperação de dados dos últimos 30 dias de forma mais ágil.

De qualquer forma, a solução de *backups* que vier a ser adquirida para o *site* secundário deverá ter a possibilidade de recuperação da informação de *backups* do *site* principal.

Caso se venha a verificar esta possibilidade de aproveitamento dos *backups* realizados no *site* principal, deverá ser implementado um processo que permita, em tempo útil, ter acesso aos suportes de *backup* realizados. O mesmo pode ser feito realizando uma réplica dos *backups* e seu armazenamento nas instalações do *site* secundário ou armazenando os suportes de *backup* do *site* principal em local seguro e independente, que em caso de desastre, permita a sua deslocação para o *site* secundário.

Para os serviços considerados críticos, alvo da análise do impacto de negócio efetuada, é impreterível garantir a sua inclusão no plano de *backup*, para proteger a informação relevante para o negócio da AMA.

Podendo, cada um dos serviços críticos ser suportado por vários servidores distintos, para se assegurar a recuperação total do serviço, é garantido que o agendamento e retenção dos *backups* definido para cada servidor, são os mesmos que os definidos para o serviço crítico. Pode dizer-se que os servidores que suportam um determinado serviço, herdam o agendamento e retenção que caracterizam esse serviço.

Seguindo o mesmo raciocínio, a proteção de um serviço é definida pelos procedimentos de proteção dos servidores que suportam esse serviço, uma vez que o serviço só está totalmente protegido, quando todos os servidores que o suportam também estão.

A recuperação de um serviço crítico implica a recuperação de todos ou parte dos servidores que suportam esse serviço, dependendo do servidor onde ocorreu a falha.

De forma a verificar que a recuperação do serviço é possível e que os procedimentos de recuperação dos servidores que suportam o serviço são adequados, é necessário executar testes de recuperação de dados de forma planeada e periódica.

Só assim, é possível garantir a capacidade de resposta da AMA, rápida e eficaz, nomeadamente em casos de emergência onde é necessário proceder à recuperação de dados, seja por motivos de eliminação acidental, corrupção, falha ou catástrofe.

É sugerido que, por cada serviço critico identificado, sejam definidos os procedimentos de execução da recuperação e um plano faseado de testes de recuperação do serviço.

Numa fase inicial é sugerido igualmente a realização de testes de todos os serviços 1 a 2 vezes por ano, até que seja constatada a efetividade e agilidade dos procedimentos. Após esta fase inicial, deve ser definida a periodicidade dos testes em função da dinâmica de cada um destes serviços.

5.4.2. Identificação de requisitos técnicos da infraestrutura de rede

Neste ponto é apresentada a análise aos vários elementos das comunicações de voz e dados, no sentido de ter uma infraestrutura redundante no *site* secundário.

A análise foi efetuada tendo em conta as necessidades de recuperação da infraestrutura e os seus serviços.

Caso a AMA pretenda assegurar uma análise das causas do desastre, potencialmente maliciosas, deverá ser também contemplado a implementação de uma solução de centralização de *logs*[28] e sua replicação à semelhança dos restantes serviços.

Não obstante a decisão de arranque poder requerer a decisão dos responsáveis, o procedimento de ativação do DRP será tanto mais simples quanto os automatismos que vierem a ser implementados, tornando-a independente de colaboradores internos ou de fornecedores. Esta presunção aplica-se também à rede de comunicações.

Propõe-se o recurso às capacidades proporcionadas pelo protocolo de *routing* BGP[29], que permite redirecionar automaticamente os pedidos, quando existir uma falha de comunicação no *site* principal. De forma a prevenir possível instabilidade de comunicações, os serviços do *site* secundário só deverão ser ativados quando necessário., no sentido de conseguir, por um lado, o suporte necessário do operador de comunicações na transição e, por outro, conseguir redimensionar as ligações.

[28] Ficheiro de registo de acontecimentos, sejam eles de segurança, ligações ou outros.

[29] *Border Gateway Protocol*, protocolo de roteamento dinâmico de comunicações entre sistemas autónomos.

A proposta de ligações a contratar para o *site* secundário é equivalente às ligações de *backup* atualmente contratadas para o *site* principal. Esta opção, em detrimento de ligações semelhantes às ligações principais do *site* principal, fundamenta-se no facto de se tratar de uma situação de contingência. Permite ter um custo de exploração mais reduzido com uma ativação imediata, que permite à AMA arrancar num cenário de recuperação de desastre com menos dependência do operador de comunicações.

Deverá ser negociado com o operador acordos de serviço que permitam repor as ligações, de acordo com um SLA que não impacte a ativação do DRP. Para tal os SLA's não deverão ser superiores a 4 horas. Este mesmo nível de serviço deve ser assegurado para eventuais redimensionamentos das ligações contratadas, que se vierem a verificar necessárias.

5.4.3. Identificação de cenários de recuperação

O cenário de Desastre (com recuperação total) considera que o *datacenter* da AMA foi comprometido, ficando inacessível, sendo necessário retomar e recuperar os serviços, a partir de um *site* secundário.

Para tal será necessário garantir, não só a disponibilização dos recursos de processamento no *site* secundário, como também a replicação e/ou recuperação dos dados entre os dois *datacenters*.

Os requisitos de implementação do *site* secundário resultam da caraterização feita ao nível da criticidade e consequentes RTO e RPO.

Foi ainda considerado um segundo cenário de recuperação, falha grave nas comunicações, que não sendo de Desastre completo comprometam as comunicações que garantem o acesso aos serviços do *datacenter* da AMA. A falha do operador de comunicações ou dos equipamentos de rede podem originar um cenário deste tipo.

Este cenário diverge do anterior pela possibilidade de possibilitar RPO's iguais ou próximos de 0, na medida que é possível recuperar os dados não replicados automaticamente (desde a última replicação até ao momento de quebra do serviço de comunicações), permitindo retomar os serviços sem perda de dados.

5.5. *Disaster Recovery Plan*

Foram desenvolvidos dois planos de recuperação: um aplica-se ao cenário de indisponibilidade do *datacenter* no caso de um desastre e o outro aplica-se ao cenário de indisponibilidade no caso de falha grave das comunicações.

O primeiro plano/cenário considera que o *datacenter* da AMA foi comprometido ficando inacessível, sendo necessário retomar e recuperar os serviços a partir do site secundário. O segundo difere bastante na medida que é possível minimizar a perda de dados (obtendo um RPO perto de 0), ao recuperar os dados existentes ativando o *site* secundário.

Estabelecem de forma semelhante um conjunto de recursos necessários para preparar uma resposta atempada a incidentes críticos e reduzir o impacto desses incidentes sobre os serviços previamente identificados.

Devido à especificidade técnica e confidencialidade de informação, representa-se de uma forma sumária a estrutura dos planos desenvolvidos (AMA, 2016c):

1. **Descrição do cenário**
2. **Definições**
3. **Âmbito de aplicação**
    - 3.1. Identificação dos serviços contemplados
4. **Estabelecimento da resposta a desastres** (identificação de requisitos e recursos necessários para responder aos incidentes)
    - 4.1. Instalação e locais
        - 4.1.1. Local de reunião da equipa de recuperação de incidentes.
        - 4.1.2. Centro de emergência - instalações alternativas para reunir a equipa de resposta a incidentes em situações de crise.
        - 4.1.3. Moradas do *datacenter* e do *site* secundário.
    - 4.2. Kit de emergência – a sua existência é importante em situações em que não é possível aceder aos SI, tornando-se essencial ter uma forma de consulta alternativa. Existe no formato físico e inclui o DRP e um telemóvel de um operador diferente das comunicações da AMA. Dada à confidencialidade dos dados que contém, deve ser garantida a sua segurança.

4.3. Equipas - constituição e contatos, necessárias à decisão e ativação do DRP:

4.3.1. Equipa de Resposta a Incidentes (ERI) – quando ativada, avalia a extensão dos danos e decide a ativação do DRP de acordo com as fases definidas.

4.3.2. Equipa de Recuperação de Desastre (ERD) – tem como principal objetivo restaurar a disponibilidade dos SI, a integridade e disponibilidade dos dados. Esta equipa é ativada a pedido da ERI.

4.3.3. Equipas de Recuperação de Serviços – tem como responsabilidade validar a recuperação e reposição dos serviços no espaço de 2 horas após a reposição da infraestrutura tecnológica e comunicações.

4.4. Contatos - internos e externos, entidades de emergência, clientes, fornecedores e parceiros que possam ser necessários no contexto da recuperação. Face ao seu conteúdo (contém dados pessoais), esta lista deve ser protegida preservando a sua confidencialidade, sendo acedida apenas pelos responsáveis das equipas ERI e ERD.

4.5. Estratégia de comunicação - consiste num plano de comunicação interna (aos colaboradores após decisão de ativação do plano) e externa (todo os que não sejam necessário para a ativação do plano, de forma a controlar a comunicação e limitar fugas de informação), tipificado nas seguintes fases:

4.6. Registo de eventos - deve ser uma constante ao longo do incidente e potencial desastre. A sua utilização permite registar informações, decisões e ações durante o período de gestão do incidente ou desastre, monitorizando o progresso para posterior análise e identificação de oportunidades de melhoria.

5. **Fases do plano** – um diagrama que representa as fases de resposta a uma emergência e ativação do DRP, detalhados nos pontos seguintes.

6. **Resposta a incidente** – desencadeado na ocorrência de um evento disruptivo no *datacenter*. O procedimento encontra-se caracterizado por uma tabela ordenada pelo número do passo, ação, responsável e tempo.
7. **Resposta a desastres** – desencadeado por indicação da ERI. Mediante o cenário, é determinada uma ordem de recuperação da infraestrutura.
8. **Reposição de serviços** – é o retorno à condição de pré-desastre, logo que possível após o encerramento de um incidente, restaurando os sistemas e operação normal dos serviços.

Anexos

No sentido de estabilizar o DRP, é recomendável o recurso a anexos para disponibilizar os formulários e tabelas de preenchimento informação durante a ativação dos planos, a informação de contexto como inventário e serviços a recuperar ou informação confidencial como os contatos e outros dados pessoais.

5.6. Execução e Monitorização

Este subcapítulo estabelece o programa a implementar pela AMA de forma a desenvolver as suas capacidades de recuperação de desastres.

O principal objetivo do programa é conceber, testar e documentar planos bem estruturados e de fácil compreensão que auxiliem a AMA a recuperar o mais rápido e eficazmente possível na eventualidade de uma ocorrência de um desastre ou emergência que resulte na interrupção do normal funcionamento dos SI alojados no *datacenter*.

Objetivos adicionais incluem a necessidade de garantir que todos os colaboradores entendem em pleno os seus deveres na implementação de um plano deste tipo, de garantir que as políticas operacionais são respeitadas dentro de todas as atividades planeadas, de assegurar que medidas de emergência propostas são eficazes em termos de custos e de considerar que possam ocorrer noutros locais da organização.

No sentido de expressar a intenção e objetivos do Conselho Diretivo, e à semelhança de um sistema de BCM (ISO 22301 – cláusula [5.3]), deve ser definida e publicada a Política de Recuperação de Desastre, que seja adequada à AMA.

É política da AMA:

- Manter uma estratégia para reagir a, e recuperar de situações de desastre, que esteja de acordo com o risco aceitável definido pelo Conselho Diretivo;
- Manter um programa de atividades que garanta que a AMA mantém a capacidade de reagir adequadamente, recuperando de situações adversas em conformidade com os objetivos de continuidade e recuperação;
- Manter os DRP adequados, suportados por um processo de escalonamento esclarecido;
- Exercitar os planos de resposta e de recuperação com base num planeamento estabelecido;
- Manter um nível de resiliência a falhas operacionais alinhado com o risco, o nível de impacto que poderia resultar da falha e do nível de risco aceitável definido pelo CD;
- Manter os colaboradores informados e sensibilizados sobre as expectativas da AMA relativamente à sua atuação durante uma situação de desastre;
- Ter em conta as necessidades de negócio e assegurar que os DRP são revistos sempre que necessário, mantendo-os atualizados, tendo em consideração alteração de circunstâncias como alterações de pessoal, dos serviços disponibilizados, etc..

O CD é a responsável por garantir a disponibilidade dos recursos necessários para a criação, implantação, operação, supervisão, avaliação, manutenção e melhoria do Programa de recuperação de desastre.

O estabelecimento deste programa permite à AMA definir planos de resposta a desastres, definindo os procedimentos necessários à sua atualização e melhoria. Para tal, são contempladas as etapas, já definidas anteriormente, de avaliação de risco e impacto no negócio e disponibilidade do plano, e definidas nesta etapa de elaboração do plano, testes, atualização, formação, monitorização e auditoria.

Os planos devem ser testados e analisados de acordo com um calendário estabelecido anualmente de modo a fornecer confiança de que irão funcionar em cenários de reais.

Os testes a realizar poderão ser totais ou parciais, de modo a validar ou exercitar determinados pontos do plano, de forma a analisar e melhorar um componente em particular.

A programação de testes pode incluir alguns exercícios que cubram partes específicas de cada plano, para analisar e melhorar este componente particular.

A AMA deve rever e atualizar regularmente os planos para manter a precisão e refletir quaisquer mudanças dentro ou fora da organização.

É necessário que o processo de atualização dos planos seja feito de forma estruturada e controlada. Sempre que sejam definidas alterações a qualquer plano é necessário assegurar que são rigorosas e devidamente testadas.

Os documentos dos planos têm que estar sujeitos a procedimentos de controlo de versões que têm que ser validadas pelo Diretor de Sistemas de Informação e Conselho Diretivo.

Alguns exemplos de alterações que requerem alteração do plano:

- Processos críticos de negócio, que origine alterações em termos de BIA
- Componentes de infraestrutura tecnológica de suporte aos serviços
- Pessoal que pertence e a equipas do plano
- Criação ou eliminação de serviços.

A realização de exercícios ou ocorrência de casos reais pode resultar na identificação de pontos de melhoria, que deverão igualmente ser incorporados numa atualização do plano.

Relativamente à formação, deve ser estabelecido um plano de sensibilização e exercício para todos os colaboradores com envolvimento nos DRP, dando-lhes o conhecimento necessário e treinando-os para a execução dos seus papéis.

A sensibilização pode ser efetuada pela apresentação do DRP, na sua implementação e posteriores alterações, enquanto os exercícios poderão corresponder aos testes a realizar aos planos, tentando envolver, no conjunto dos testes a realizar, o maior número de pessoas.

6. Resultados

Pretende-se neste capítulo avaliar se as diretrizes identificadas são suficientes para a elaboração de um BCP, através de uma análise comparativa ao plano desenvolvido pela organização alvo de estudo.

Além da pertinência da necessidade de um plano de continuidade em qualquer organização, constata-se a preocupação e a sensibilização deste tema em entidades governamentais e pela gestão de topo, através dos programas governamentais em melhorar o serviço prestado aos cidadãos, em acompanhar a comunidade europeia nas boas práticas de segurança da informação e pela imagem da organização.

Esta nova cultura organizacional torna-se um fator essencial para a implementação de um sistema BCM, que garanta a continuidade do negócio em caso de uma disrupção, melhorando a qualidade dos serviços que a AMA presta aos seus parceiros ministeriais e cidadãos.

6.1. Análise crítica

Constata-se que a metodologia usada para desenvolver o BCP e respetivo DRP estão de alinhados com os *standards* internacionais contendo alguns elementos comuns:

- Usa uma metodologia adaptada do PDCA
- Foi executado um levantamento exaustivo dos serviços e processos de negócio
- Foi desenvolvida uma política que aumenta a resiliência da AMA e que envolve todos os colaboradores
- Contempla um programa de monitorização e atualização do BCP e DRP
- A solução de recuperação garante um estado de prontidão da infraestrutura tecnológica

É notório em todo o desenvolvimento do plano de continuidade, além das referências aos *standards*, as boas práticas de *frameworks* de gestão de serviços e *governance*.

Verifica-se o alinhamento com processos ITIL no que toca às boas práticas de gestão de serviços (gestão de continuidade, disponibilidade e de alteração), bem como o recurso à arquitetura empresarial para mapear as relações entre a camada tecnológica, aplicacional, processos e pessoas.

Esta arquitetura permite quantificar e qualificar o impacto no negócio, determinando uma estratégia adequada de recuperação de processos de negócio realmente críticos à organização.

Além da metodologia PDCA do ISO 22301 usada para a elaboração do BCP, constata-se o recurso ao ISO 27005 para identificar as ameaças e desenvolver a matriz de avaliação do risco.

É com base na análise de impacto no negócio, que é desenvolvida a respetiva estratégia de recuperação dos processos críticos do negócio.

Os restantes *standards* são tidos em conta, mas com menor relevância que os anteriores, desde a prontidão das TIC (ISO 27031), gestão do risco (ISO 31000), à gestão da segurança da informação (ISO 27001).

Esta situação é óbvia quando não se certifica, mas a integração e relação entre *standards* está sempre presente.

O *datacenter* da AMA encontra-se em *hosting* bem como usa um sistema partilhado de *backups*, pelo que o plano de continuidade e recuperação deve obrigatoriamente contemplar o fornecedor/parceiro desta infraestrutura física. O plano acaba por ser inadequado na solução de *backup/restore*.

Outros fatores, nomeadamente de segurança e controlo de acessos ao *datacenter* que dependem o fornecedor dessa infraestrutura, colocam em causa os tempos de resposta à avaliação e resolução do evento disruptivo. Por exemplo, uma falha de comunicações que se não for resolvida em duas horas, o *site* secundário é ativado obrigando a toda a replicação de dados que por sua vez pode levar mais algumas horas, em que é necessário a intervenção (seja contatos, controlos de acesso, e outros controlos definidos na ISO 27002) da equipa técnica responsável pelo *datacenter* e solução de *backups*.

Outra situação inexistente é a segurança no *site* secundário, seja das instalações como de toda a infraestrutura tecnológica que tem uma réplica dos dados do negócio.

Obviamente o plano desenvolvido tem algumas lacunas, não só pela limitação temporal para a sua elaboração, mas também pelas restrições orçamentais. Estes dois fatores limitam assim a estratégia e a solução de recuperação.

As limitações financeiras não permitiram a implementação do BCP e respetivo DRP. Apesar de estarem alinhados com as boas práticas e *standards* internacionais

nomeadamente com o ISO 22301, não é possível avaliar se os planos desenvolvidos são os adequados à organização.

Assim, este plano de continuidade e recuperação de negócio deve ser revisto aquando da luz verde financeira, bem como permitir um ajuste do catálogo de serviços existente à data da sua implementação e respetiva solução de recuperação.

Estes planos requerem testes, manutenções, revisões e auditorias periódicas, como processo de melhoria contínua e de forma a garantir que é adequado à organização e a novos processos de negócio.

No momento que se implemente um BCP e respetivo DRP, tanto os planos como as soluções de recuperação, têm um custo superior de manutenção e suporte, mas revelam-se essenciais na recuperação de um evento disruptivo que pode ter uma consequência grave muito superior ao investimento feito.

Alguns destes serviços não são mensuráveis, mas têm um impacto muito alto e severo na organização, pelo que qualquer investimento na gestão do risco, da continuidade de negócio e segurança da informação (mesmo que uma solução não certificada, mas devidamente alinhada com os *standards*), é sempre uma garantia e forma de minimizar um impacto nos processos de negócio.

6.2. Recomendações

São diversos os fatores sobre os quais as organizações não têm o controlo absoluto, por isso, a criticidade do negócio e outros fatores já indicados, levaram à elaboração de um plano de continuidade e recuperação que permitisse que a organização cumprisse os objetivos a que se tinha proposto.

As organizações nem sempre utilizam uma abordagem sistemática na elaboração dos planos o que resulta em iniciativas isoladas e na implementação de soluções parciais. Para que tal não aconteça, recomenda-se a manutenção dos planos até à disponibilidade orçamental da AMA, também com o intuito de manter viva a cultural organizacional referente à continuidade do negócio e segurança da informação, e que de alguma forma o investimento feito no BCP inicial não seja em vão.

Recomenda-se igualmente estratégias de recuperação alternativas com um custo inferior, ou seja, uma análise custo-benefício para as diversas opções que permitam selecionar as medidas adequadas ao negócio e organização.

No entanto, existem alguns pontos a melhorar ou a adicionar por serem omissos:

- Integração do ISO 27001 no *site* secundário
- Os cenários avaliados são demasiado genéricos, o que não permite uma análise profunda das vulnerabilidades
- Integrar o parceiro responsável pelo *datacenter* e pelo sistema partilhado de *backups* no plano de continuidade e recuperação
- A política de comunicação está contemplada, mas precisa de ser melhorada
- O custo da solução de recuperação é demasiado alto, colocando em risco a sua implementação (deviam ter analisado outras alternativas como por exemplo uma solução IaaS[30] ou SaaS[31])
- Certificação do sistema BCM - ISO 22301
- Certificação ISO 27001
- Implementação ITIL na organização

Estas situações podem ocorrer em sistemas BCM e planos não certificados, ou em soluções de recuperação que não sejam adequadas à organização devido a restrições financeiras, técnicas, legais, entre outras.

Os planos foram elaborados e implementados de acordo com os *standards* e as melhores práticas, mas as limitações financeiras e temporais deste projeto não permitem a sua certificação. Não só pelo seu custo, mas pelos requisitos de medidas a aplicar exigidas pela certificação, que implica também uma infraestrutura tecnológica alternativa e de todo o SGSI a implementar em ambos os *datacenter*.

A não certificação do plano prende-se igualmente pelo tempo limitado que a AMA tem para implementar um BCP. Por haver necessidade, desenvolveu-se o plano não certificado, mas alinhado com as diretrizes identificadas, tidas como adequadas e suficientes para a elaboração de um plano de continuidade e recuperação adequado às necessidades da organização e dos processos críticos do negócio.

[30] *Infrastructure as a Service* – tipologia de serviços baseada em *hosting*.
[31] *Software as a Service* – aplicações fornecidas por terceiros via web .

7. Conclusão e Perspetivas de Trabalho Futuro

A continuidade de negócio é um processo contínuo, com o objetivo de garantir que a organização funciona de forma eficiente, tanto em tempos normais como em tempos turbulentos. Para tal, implica ter um sistema de BCM robusto, continuamente testado e atualizado de acordo com as necessidades do negócio.

As organizações que agora começam a dar relevo à continuidade de negócio, tendem a concentrar os seus esforços dentro das suas próprias fronteiras, ignorando as vulnerabilidades e ameaças representadas pelos seus fornecedores e parceiros.

As diretrizes e *frameworks* apresentadas neste documento são suficientes e adequadas para o desenvolvimento de um BCP, alinhado com as necessidades da organização e eficiente para garantir a operação do negócio no caso de um evento disruptivo. Servem para negócios exclusivos (se a necessidade é pontual e imediata) e para o planeamento de um sistema de gestão de continuidade de negócios total e completo (incluindo os fornecedores, parceiros e clientes).

É possível desenvolver um plano de continuidade e recuperação sem seguir as linhas orientadores e *standards* identificados neste estudo. No entanto, uma solução certificada ou orientada por estas normas e metodologias, apresentam benefícios superiores na implementação e integração com terceiros, na facilidade de gestão da política de continuidade, na construção uniformizada de relatórios (para análise e avaliação dos riscos e melhoria contínua) e numa segurança de informação robusta, adequada e de acordo com as práticas internacionalmente aceites.

A política de continuidade em Portugal tem pouca expressão, com apenas 3 certificações de sistemas BCM e apenas dois organismos públicos com o BCP em progresso (incluindo a AMA). A investigação demonstra a necessidade de desenvolvimento de um BCP, os benefícios que podem advir da existência de um plano de recuperação e a garantir que a organização continua a operar após um incidente ou desastre.

A sobrevivência e a sustentabilidade das organizações constroem-se com um processo contínuo de identificação de vulnerabilidade e ameaças, minimização dos riscos e impactos que estes têm no negócio, de envolvência de todos os intervenientes e da criação de uma cultura de continuidade, gestão do risco e segurança da informação no negócio.

7.1. Perspetivas de Trabalho Futuro

Após a elaboração do BCP, a equipa de projeto encontra-se a identificar os donos dos serviços de negócio, a criar e identificar as equipas responsáveis pela ativação e execução dos planos.

Existe ainda algum trabalho de *backoffice* na catalogação dos serviços e processos de negócio e respetivas dependências e relações, respeitando as boas práticas do ITIL v3 e de arquitetura empresarial.

A solução de recuperação não tem previsão de implementação pois implica a construção de um *site* secundário e de uma infraestrutura de comunicações de voz e dados redundantes. Tal solução implica aquisição de serviços de comunicações e infraestruturas tecnológicas para garantir uma réplica sincronizada do *datacenter*, pelo que se encontra dependente do orçamento da AMA e da respetiva autorização do Governo para o investimento.

Existe ainda um trabalho futuro de medir o risco e o custo de oportunidade na definição dos serviços críticos, das vantagens e desvantagens da solução e da perda de dados versus disponibilidade.

A infraestrutura da AMA é muito volátil, com o aparecimento constante de novos serviços, sistemas, plataformas e projetos variados, exigindo a monitorização e controlo constante, bem como ajustes ao plano de continuidade e recuperação. O crescimento da infraestrutura e a renovação tecnológica, obriga igualmente a testes periódicos de forma a garantir que as soluções de recuperação estão operacionais, são adequadas aos novos sistemas e estão alinhados com os novos processos de negócio.

A manutenção do BCP deve prever também a mudança do mapa de pessoal. Além da manutenção dos serviços, processos de negócio e tecnologia que a suporta, deve existir um trabalho futuro de formação e reciclagem dos elementos das equipas de recuperação. Deve-se igualmente incutir uma cultura de continuidade e gestão de risco em todos os organismos parceiros da AMA.

Referências Bibliográficas

Aggarwal, R. (1 de novembro de 2015). *What is RPO, RTO, WRT, MTD?* Obtido de Virtualization the Future: http://virtualization24x7.blogspot.pt/2015/11/what-is-rpo-rto-wrt-mtd.html

AMA. (novembro de 2014). *Plano de Atividades.* Obtido de AMA: https://www.ama.gov.pt/documents/24077/28687/ama_pa_2015.pdf/f8f1c016-7a5f-453d-b2b7-5a368067b077

AMA. (9 de março de 2015). PGPRIC. Obtido de AMA: https://www.ama.gov.pt/documents/24077/28645/Plano_PGPRIC.pdf/bd69ac65-26f0-43c2-9be1-65bc360436a1

AMA. (2016a). *AMA*. Obtido de AMA: https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/a-ama

AMA. (2016b). *Competências*. Obtido de AMA: https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/competencias

AMA. (2016c). Programa de Recuperação de Desastre dos Serviços IT do Centro de Processamento de Dados da Agência para a Modernização Administrativa. Lisboa.

Caetano, A. (Abril de 2013). Engenharia Empresarial. Lisboa.

Crawford, S. (outubro de 1983). *The Origin and Development of a Concept: The Information Society*. Washington University, School of Medicine Library, St. Louis, Missouri, United States of America: Bull. Med. Libr. Assoc.

Dobler, M. (2005). *National and international developments in risk reporting: May the German Accounting Standard 5 lead the way internationally?* Obtido de German Law Journal: http://www.germanlawjournal.com/volume-06-no-08/

Gartner. (31 de julho de 2016). *Digital Risk Security*. Obtido de Gartner: http://www.gartner.com/technology/topics/digital-risk-security.jsp

Gasiorowski-Denis, E. (12 de junho de 2012). *Business continuity - ISO 22301 when things go seriously wrong*. Obtido de ISO.org: http://www.iso.org/iso/news.htm?refid=Ref1602

IRM. (2002). *A Risk Management Standard.* Obtido de The Institute of Risk Management: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

ISACA. (2012). *What is COBIT 5?* Obtido de ISACA: http://sas-origin.onstreammedia.com/origin/isaca/COBIT/COBIT5-Tool-Kit.zip

IsecT Ltd. (2016). *ISO/IEC 27001*. Obtido de iso27001security: http://www.iso27001security.com/html/27001.html

ISO. (2014). *ISO Survey*. Obtido de ISO: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF

ISO 22301:2012. (s.d.). Societal security — Business continuity management - Requirements. *Societal security — Business continuity management systems - Requirements*. ISO. Obtido de www.iso.org.

ISO 24762:2008. (s.d.). Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services.

ISO 25010:2011. (s.d.). Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models.

ISO 27001:2013. (s.d.). Information technology -- Security techniques -- Information security management systems -- Requirements.

ISO 27002:2013. (s.d.). Information technology -- Security techniques -- Code of practice for information security controls.

ISO 27005:2011. (s.d.). Information technology -- Security techniques -- Information security risk management.

ISO 27031:2011. (s.d.). Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity.

ISO 31000:2009. (s.d.). Risk management -- Principles and guidelines.

ISO 42010:2011. (s.d.). Systems and software engineering — Architecture description.

ITIL and ITSM World. (dezembro de 2005). *ISO 20000, BS15000 and ITIL*. Obtido de The ITIL and ITSM World: http://www.itil-itsm-world.com/itsm-kit.htm

ITSMF. (2010). ITIL. *Diagrama de Gestão de Serviços ITIL*. ITSMF.

Laudon, K. C., & Laudon, J. P. (2012). *Management Information Systems* (12th ed.). England: Pearson.

Matos, J. A. (2009). *Dicionário de Informática e Novas Tecnologias.* Lisboa: FCA.

Mundo ITIL. (2016). *ITIL Foundation*. Obtido de Mundo ITIL: http://www.mundoitil.com.br/itil-foundation/

Teixeira, S. (2005). *Gestão das Organizações.* McGrawHill.

Varajão, J. (2005). *Arquitectura da Gestão de Sistemas de Informação.* FCA.