Paulino Joaquim Ferreira dos Santos

Plano de Continuidade de Negócio

Orientador: Prof. Doutor Rui Ribeiro

Universidade Lusófona de Humanidades e Tecnologias

Escola de Comunicação, Arquitetura, Artes e Tecnologias da Informação

ECATI

Lisboa

2019

Paulino Joaquim Ferreira dos Santos

Plano de Continuidade de Negócio

Dissertação defendida em Provas Públicas na Universidade de Humanidades e Tecnologias, para a obtenção do Grau de Mestre em Engenharia Informática e Sistemas de Informação, no curso de Mestrado em Engenharia Informática e Sistemas de Informação, no dia 31 de Outubro de 2019, perante o júri, nomeado pelo Despacho de Nomeação de Júri nº 220/2019, de 11 de Setembro de 2019, com a seguinte composição:

Presidente: Professor Doutor José Luís Azevedo Quintino Rogado

Arguente: Professor Doutor Nuno Manuel Garcia dos Santos (UBI)

Orientador: Professor Doutor Rui Pedro Nobre Ribeiro

Universidade Lusófona de Humanidades e Tecnologias

Escola de Comunicação, Arquitetura, Artes e Tecnologias da Informação

ECATI

Lisboa

2019

Dedico este trabalho à minha família.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.

Martin Luther King

Agradecimentos

Terminada uma etapa tão importante na minha vida pessoal e profissional, com a finalização desta Dissertação, não posso deixar de agradecer a todos aqueles que fizeram parte do meu percurso, que me apoiaram e que permitiram que este trabalho fosse possível.

É de salientar, em primeiro lugar, a Universidade Lusófona de Humanidades e Tecnologias nomeadamente, Professor Doutor Rui Ribeiro meu tutor e ao PhD. José Rogado a quem agradeço a oportunidade que me foi proporcionada ao integrar-me nesta instituição.

Agradeço a todo o corpo docente e não docente pelo cuidado demonstrado.

Agradeço aos Professores Doutores Sérgio Guerreiro, Alexandra Campos, José dos Santos, Maria da Costa, Sofia Azevedo e Diamantino Costa a orientação e o apoio concedido em todas as questões levantadas ao longo deste Mestrado, que tanto contribuíram para melhorar a minha prática no sentido da reflexão.

Não posso deixar de mencionar os meus Pais, os meus irmãos, pelo apoio durante os meus estudos, Libana Marcelino e Rode Afonso e aos meus colegas do curso Adilson Morgado e Yuri Van-dunén a quem agradeço terem feito parte da minha vida académica e hoje tenho como amigos.

A todos os que me apoiaram e incentivaram, para que este sonho torna-se em realidade.

RESUMO

Com grande regularidade somos confrontados com notícias de tempestades, terramotos, incêndios, falências, crises, com impacto nas pessoas e nas organizações. Catástrofes como a plataforma petrolífera no Golfo do México, ou impacto do vulcão Islandês Eyjafjallajökull na circulação aérea pelas suas consequências diretas e indiretas alerta-nos para a necessidade de desenvolvimento de uma política de gestão de continuidade de negócio que auxilie as organizações e minimize os seus impactos, para evitar a ocorrência de catástrofes. A gestão de continuidade de negócio tem como objetivo principal evitar, ou reduzir sensivelmente, as perdas das organizações, em caso de incidentes, que afetam as suas operações, além de restaurar as suas atividades num espaço de tempo cada vez mais reduzido. A política de gestão continuidade de negócio é seguida com grande cuidado no mundo anglo-saxónico, mas não é seguida na generalidade das organizações portuguesas, com a exceção das empresas de grande dimensão dos sectores financeiros, de seguros e de telecomunicações.

No já referido contexto é claramente a resiliência e administração a mudanças imprevisíveis, dentro das TI e ecossistemas de negócio, são elementos fundamentais para garantir a segurança de uma empresa. Os objetivos chave precisam de estar alinhados com a continuidade dos seus processos-chave no caso de um incidente perturbador. Claramente que um plano de continuidade de negócios bem estruturado (*Business Continuity Plan* BCP), em conformidade com uma visão ampla da empresa, ou seja, um plano de cobertura de todas as áreas da empresa, a fim de atingir o objetivo de manter e restruturar as operações críticas. Estratégias de recuperação de desastres devem ser bem tratadas e apoiar todas as atividades de continuidade de negócios. Identificar e enfrentar esses desafios e a meta da continuidade de negócios (*Business Continuity Plan* BCP). O objetivo deste estudo é analisar os principais vetores apresentar os requisitos organizacionais e bases conceptuais, mais especificamente sobre a continuidade dos negócios e conceitos de recuperação de desastres. Aspetos fundamentais com as melhores práticas reais de gestão de planos contínuos de negócio.

Palavras-Chave: Continuidade de Negócio; Transações de Negócio; Terceirização de Processos de Negócios; Análise de Impacto nos Negócios; Recuperação de Desastres.

ABSTRACT

With great regularity we are faced with news of storms, earthquakes, fires, bankruptcies, crises, impacting on people and organizations. Disasters like oil platform in Mexico Golf or impact of the Icelandic volcano Eyjafjallajökull in the area circulation by, their direct and indirect result alerts us to the existence of a business continuity management policy, that helps organizations minimize impacts.

Business continuity management aims to avoid or substantially reduce the losses of organizations in the event of incidents that affect their operations and restore its activities in time as short as possible. This policy is followed with great care in the Anglo-Saxon world but didn't accompanied in most Portuguese companies, excluding large enterprises in the financial sector, insurance and telecommunications.

In this context the resilience and manage unpredictable changes within the IT and business ecosystems are essential to make sure the security of a company. These key objectives must be aligned with the continuity of its key processes in the case of a disturbing incident. For this, they need to have a continuity plan well-structured business (Business Continuity Plan BCP), which is in line with a broad view of the company, i.e. a coverage plan for all areas of the company in order to achieve objective of maintaining and redesigning the critical operations. Disaster recovery strategies should be treated well and support all business continuity activities. Identify and address these challenges and the goal of business continuity (BCP Business Continuity Plan). The aim of this study is to analyse the main vectors presented state of the art of organizational requirements and conceptual bases, more specifically on business continuity and disaster recovery concepts. Fundamental aspect with the best real practice of business continuity management plan.

Keyword: Business Continuity, Business Transactions, Business Process Outsourcing, Impact Analysis in Business, Disaster Recovery.

Abreviaturas e Símbolos

A/C - Ar Condicionado

BC - Business Continuity

BCM - Business Continuity Management

BCMS - Business Continuity Management Systems

BCI - Business Continuity Institute

BCI - British Standards Institution

BGP - Border Gateway Protocol

BIA - Business Impact Analysis

BPC - Business Plan Continuity

BS - Business Standards

CPD - Centro de Processamento de Dados

COBIT - Control Objectives for Information and Related Technologies

DMZ - Demilitarized Zone

DR - Disaster Recovery

DRP - Disaster Recovery Plan

FTP - File Transport Protocol

GB - Gigabyte

GCN - Gestão de Continuidade de Negócio

HVAC - Heating Ventilating and Air Conditioning

IEC - International Electrotechnical Commission

INE - Instituto Nacional de Estatística

ISO - Internacional Organization Standardization

IT - Information Technology

ITIL - Information Technology Infrastructure Library

LAN - Local Architecture Network

MTTR - Mean Time to Repair

MTBF - Mean Time Between Failures

MAR - Modelo de Avaliação de Risco

MTD - Maximum Tolerable Downtime / Tempo Máximo Tolerável de Inatividade

MTPOD – Periodo Tolereble Period of Disruption

NIST - National Institute of Standards and Technology

PCN - Plano de continuidade de negócio

PDCA - Plan Do Check Act

PECB - Professional Evaluation and Certification Board

PRD - Plano de Recuperação de Desastres

PMBOK - Project Management Body of Knowledge

RPO - Recovery Point Objective

RTO - Recovery Time Objective

SAN - Storage Area Network

SDLC - System Development Life Cycle

SI - Sistemas de Informação

SQL - Structured Query Language

SMS - Short message Service

TI - Tecnologias da Informação

UPS - Uninterruptible Power Supply

VPN -Virtual Private Network

WAN - Wide Area Network

Índice

Índice de Tabelas

Índice de Figuras

INTRODUÇÃO

1.1 PROBLEMA

A continuidade do negócio e recuperação de desastre no ponto de vista global, tendências e desafios.

Em comparação com outras disciplinas de gestão empresarial, o conceito de continuidade de negócios é relativamente novo. Criado na década de 1960 como IT *disaster recovery*, "recuperação de desastre", esta disciplina ganhou notoriedade com o ataque terrorista no ano de 2001 no dia 11 de setembro na cidade de Nova York, mais recentemente com a última vaga do Estado Islâmico (ISIS) nos ataques terroristas. Devido esta alavancagem de risco, este tema é agora regularmente debatido em salas de reuniões e cenários empresariais com dimensão global. Entretanto, ainda não existem sociedades eficazes para medir objetivamente e de forma consciente o nível de prontidão da organização para catástrofes ou estados de preparação para desastres (Vistual Corporation, 2007). A continuidade de negócio e a recuperação de desastres de TI, pode significar a diferença entre a vida e a morte para uma empresa, juntos eles podem significar a diferença em colapso nas diversidades ou serem capazes de garantir a continuidade do negócio (Business Continuity, 2016).

A indústria da tecnologia de informação tem avançado rapidamente ao longo dos anos sendo atualmente um componente vital para a realização de negócios (Botha and Solms, 2004).

Atualmente, os indivíduos e as empresas são cada vez mais dependentes da tecnologia de informação, na medida em que é difícil encontrar uma empresa que não tenha tecnologia, a maioria das empresas não operam sem sistemas de informação (Barbara, 2006).

Os sistemas da tecnologia de informação evoluíram e há necessidade de proteção contra as possíveis ameaças as informações que processa, transmite e armazena.

Neste contexto, qualquer falha ou desastre no sistema da tecnologia de informação poderia ter sérias consequências para uma empresa (Botha e Solms, 2004) e como resultado, de acordo com a maioria dessas empresas nesses sistemas, nenhuma empresa pode ignorar a necessidade de uma continuidade de negócio e de um planeamento de recuperação de desastres, independentemente da dimensão da empresa, das receitas, ou do número de funcionários, bem

como a necessidade de planear para a potencial interrupção de serviços de tecnologias tem aumentado exponencialmente em negócio de continuidade, de recuperação de desastres. O planeamento tornou-se imperativo (Snedarker, 2007).

Da análise considera-se que o PCN tem os seguintes princípios:

- É um princípio de gestão de capacidade de uma organização para conseguir manter um nível de funcionamento adequado até ao retorno normal, após a ocorrência de incidentes e interrupção de negócios críticos.

- É um princípio que deve ser desenvolvido previamente a partir de um conjunto de estratégias e planos táticos, capazes de permitir o planeamento e a garantia dos serviços essenciais, devidamente identificados e preservados. O PCN a partir desse conjunto de estratégias e processos orienta e define como e quais as ações que devem ser executadas para que se construa uma resiliência organizacional de resposta para salvaguarda dos negócios (Plano de continuidade de negócio, 2012).

- É um princípio desenvolvido evitar a interrupção ao normal funcionamento do negócio. Se esses eventos não podem ser evitados, as metas do plano servem para minimizar a interrupção e reduzir o dano potencial que tais interrupções podem custar à organização.

- É um princípio que também deve ser projetado para minimizar o custo associado com os eventos perturbadores e mitigar os riscos associados a esses eventos perturbadores (Gregg, 2007). O planeamento de continuidade de negócio envolve o desenvolvimento de um conjunto de procedimentos para as diversas unidades de negócio que irá garantir a continuidade do processo crítico de negócio, enquanto o centro de dados recupera do desastre (Wilson, 2000).

O desastre é um evento catastrófico resultante de causas naturais, ou do ser humano, que afeta seriamente, ou impende totalmente, a continuidade normal das operações. A continuidade dos negócios, estabelece as estratégias, os procedimentos e as ações críticas necessárias para responder e administrar uma situação de crise (Tucker, 2014). O PCN também mostra, como uma organização responde aos desastres inesperados, às interrupções ou alterações (COBIT, 2013). Uma crise pode ser um desastre natural, uma catástrofe, ou pode ser apenas um simples

acidente, que pode causar uma interrupção de um ou mais serviços, com perda parcial ou total do negócio (ISO22301, 2012) (Heng, 2007).

A British Standards Institution define *Business Continuity* (BC) como a "capacidade da organização para continuar a entrega de produtos ou serviços em níveis predefinidos aceitáveis após um evento perturbador". Ele também define Gestão de Continuidade de Negócio (GCN), ou ***Businesss Continuity Managment (BCM),*** como um processo de gestão holística que identifica as potenciais ameaças para a organização e para os impactos que podem causar essas ameaças nas operações de negócios, proporcionando uma estrutura adequada para a construção de uma resiliência organizacional com a capacidade para uma resposta eficaz que salvaguarde os interesses dos seus principais intervenientes nomeadamente: a reputação, a marca e as atividades de criação de valor (ISO22301, 2012). O the British Contituity Institute (BCI, 2009) afirma que o objetivo de um plano de continuidade de negócios é fornecer uma estrutura, e processos documentados, para permitir que a organização retome todos os processos de negócio dentro do seu objetivo de tempo de recuperação após um incidente perturbador.

Tendo este conjunto de objetivos em mente, é fundamental ter uma visão completa da organização, e um plano concreto e consistente que garante a integridade da missão e estratégia da organização, e assegurar a continuidade da operação. Para isso, é necessário criar um mapa completo de todos os processos críticos, e não críticos, de uma empresa para ter uma organização, e se necessário replicadas num ambiente diferente. Eles vão retomar os processos mapeados em ordem para reconstruir operações vitais e assegurar a retomada das operações e serviços sensíveis ao tempo em caso de emergência, dentro de um curto período. Portanto, a definição de todo o processo crítico e elementos necessários para executar estas tarefas fundamentais são importantes para garantir a continuidade do negócio e ter resiliência organizacional (Hiles, 2010).

Um dos principais desafios para implementar um Businesse Plan Continuity (BPC) *in-house* e Disaster Recovery Plan (DRP) é estabelecer um conhecimento necessário sobre todos os recursos-chave, ou atividades-chave e elemento-chave da organização. Por exemplo, após um evento perturbador, uma organização precisa estabelecer processos de *redesign* e reengenharia, a fim de adaptar os seus negócios para novas realidades. Assim, perante uma crise é pertinente que uma empresa adote uma metodologia estruturada e um conjunto de ferramentas que permita a alteração e a adaptação dos seus processos para que as operações da empresa

continuem a trabalhar, com os seus recursos disponíveis existentes, mesmo com uma capacidade parcial de produção.

1.2 **OBJETIVO GERAL**

O objetivo do plano de continuidade do negócio é especificar as ameaças e riscos identificados nas organizações e analisar o impacto no negócio, caso essas ameaças se concretizem. Visa com isso tornar possível o funcionamento de uma organização num nível aceitável em situações de contingência, resguardando os interesses dos intervenientes, a reputação, a imagem da organização e suas atividades afins de significativo valor agregado.

Tendo em conta a revisão da literatura surgem as seguintes questões de investigação:

- Como colocar em prática, de modo operacional, um plano de continuidade de negócio?
- Como pode ser operacionalizado um plano de continuidade de negócio?
- Quais os processos de negócio extremamente críticos e estratégicos para a organização?
- Qual a solução tecnológica, com menor custo, que se alinha aos parâmetros definidos nos objetivos específicos?

Para responder à questão de investigação foram identificados alguns objetivos.

- Definir o processo de implementação.
- Definir as tecnologias utilizadas e a sua implantação.
- Definir os processos de monotorização.
- Definir a envolvência da gestão de topo no projeto.
- Verificar de que modo esta estratégia está alinhada com a atividade.

1.3.2 **OBJETIVO ESPECÍFICO**

Escolher o cenário tecnológico de recuperação de desastres que melhor se adapte à Organização considerando os seguintes parâmetros:

O plano de continuidade de negócio é uma ferramenta essencial que visa garantir que a empresa está preparada para uma recuperação imediata das suas atividades críticas e dos seus interesses de apoio e aplicações em caso de um desastre. Ambos os planos (BCP) (DRP) descrevem as ações a ser implementadas, os recursos necessários e os procedimentos, antes durante e após um desastre. Os planos são projetados para minimizar os impactos em termos de recursos humanos, operacionais de impacto financeiro inerente a uma situação de desastre.

Os principais objetivos do BCP e do DRP segundo Cobit são os seguintes: (COBIT, 2013) (ISO22301, 2012) (Hiles & Noakes-Fry, 2014)

- Definir as diretrizes para garantir a segurança dos trabalhadores;
- Minimizar o tempo de inatividade e perda de dados;
- Proteger e impedir a organização, no caso em que a totalidade ou parte de suas operações e/ou serviços de computação de se tornarem inutilizáveis;
- Desenvolver estratégias de recuperação;
- Identificar medidas de prevenção;
- Preparações de ações antecipadas a serem tomadas em resposta a possíveis perturbações ou desastres;
- Abordar o potencial impacto de diferentes níveis de perturbações;
- Certifica-se de que o negócio vai continuar a oferecer serviços críticos;
- Certifique-se que o serviço vai sobreviver a um evento desastroso.

Assim o plano de continuidade de negócio precisa de garantir uma resposta rápida e eficaz para o inesperado através de um quadro de ações, de procedimentos e de protocolos capazes de gerir uma perturbação grave das atividades (*Severe Business Disruption* SBD). Por essa razão há uma necessidade de assegurar que existem formas pré-definidas para medir e estabelecer métricas em causas objetivas, relacionando-as tanto com o desempenho do programa como com a capacidade de recuperação da organização.

No já referido contexto o objetivo é a criação de uma nova metodologia e estrutura para construir uma BCP e DRP, portanto, este é o passo para se apresentar um estado de arte dos requisitos organizacionais e das bases conceptuais, particularmente sobre a continuidade de negócios e conceitos de recuperação de desastre bem como alguns *insight*s recolhidos das principais partes interessadas e gestores nas organizações.

1.3 **ORGANIZAÇÃO**

No início a perspetiva da gestão estratégica é caracterizada como um processo de um longo prazo para o desenvolvimento de um compromisso continuo com a missão e visão da organização, alimentado uma cultura que identifica e apoia a missão e visão da organização, mantendo o foco claro sobre a organização da agenda estratégica em todos os seus processos e atividades de decisão (Choi, 2009). Steiss (1985) vê a gestão estratégica como o processo pelo qual as metas e objetivos identificados, as políticas são formuladas e as estratégias são selecionadas, a fim de alcançar os objetivos globais ou missão de uma organização.

Um aspeto importante da gestão estratégica é a sua enfase na organização e a adaptação a exigências e ambientes (Choi, 2009).

2. REVISÃO BIBLIOGRÁFICA

Segundo a norma ISO 22301 (ISO 22301, 2012) a gestão da continuidade de negócio é um procedimento abrangente que reconhece potenciais ameaças à organização e os seus impactos nas operações, que fornece uma estrutura para a criação de organizações com maior nível de invulnerabilidade, com maior capacidade de resistência e com capacidade real de resposta eficiente que garante os interesses dos seus acionistas e das partes interessadas envolvidas, assim como salvaguarda a sua reputação, a sua marca e as suas atividades de criação de valor.

Já para o BCM Institute (BCM Institute, 2014) é uma matéria que envolve a totalidade da organização e um conjunto de procedimentos que reconhece potenciais impactos que podem ameaçar a organização. Oferece uma capacidade de resposta eficiente que garante a salvaguarda dos principais interessados, acionistas e partes interessadas, e da sua reputação (nome e imagem).

Segundo a norma ISO 22301 (ISO 22301, 2012) a gestão de continuidade de negócio deve considerar a importância dos pontos referidos na Tabela 1 que se segue.

Ponto	Descrição
Ponto 1	Compreender as necessidades da organização e a necessidade para a criação de um plano de continuidade de negócio as suas políticas e objetivos.
Ponto 2	Implementar controlos e métricas de forma a medir a capacidade global da organização de resposta a incidentes disruptivos.
Ponto 3	Monitorizar a performance e a efetividade do plano de continuidade de negócio.
Ponto 4	Melhoria continua baseada na avaliação dos objetivos.

Tabela 1: Pontos-Chave de um Plano de Continuidade de Negócio

Fonte: (ISO 22301, 2012)

Para que a gestão da continuidade de negócio atinga o sucesso é essencial a envolvência e o apoio da gestão de topo da organização. O melhor modo de beneficiar desse apoio é salientar os benefícios de possuir um processo de gestão de continuidade de negócio

eficiente. Atualmente uma adequada gestão de continuidade de negócio não implica tomar decisões para dirigir e remeter questões externas, no entanto implica reconhecer o valor acrescentado que as práticas eficientes de gestão de continuidade de negócio acrescentam à organização (St-GERMAIN)

- Salvaguarda do valor da organização favorecendo os acionistas.
- Compreensão superior do negócio resultante da análise de riscos.
- Superação operacional decorrente da redução de risco.
- Diminuição de *downtime* através da identificação de *workarounds* para abrandar as interrupções.
- Identificação de questões de conformidade para outros processos.
- Registos pertinentes para a organização devem ser mantidos e preservados.
- Considerar as questões da legislação, de segurança e saúde.
- Melhoramento operacional por meio da reengenharia de processos de negócio.
- Salvaguarda dos ativos físicos e do conhecimento do negócio.
- Proteção dos mercados assegurando a continuidade da atividade.
- Melhoramento da segurança geral.

2.1 **PLANO DE CONTINUIDADE DE NEGÓCIO (PCN)**

Um dos factos que alertou a atenção das organizações para planos de recuperação de desastres e continuidade de negócio foi o atentado terrorista do onze de setembro às Torres Gémeas em 2001. Atualmente, em Portugal sobretudo em organizações de maior dimensão, parece já existir uma consciencialização relativa aos riscos de perdas de dados de negócio que, claramente, conduz as organizações a uma preocupação sobre a necessidade de prevenção desses riscos (BdP, CMVM, CNSF, 2017). Para iniciar a preparação do Plano de Continuidade do Negócio é necessário que os responsáveis internos da organização conheçam o conceito e o seu valor assumindo-o como um compromisso essencial para a prevenção e preservação das organizações. Embora, atualmente, os responsáveis internos da organização conheçam o conceito do plano de continuidade de negócio ainda não o assumem como uma ferramenta essencial. A capacidade das organizações recuperarem rapidamente de um desastre natural está na disponibilização de soluções de recuperação de sistemas de informação crítica sem os quais

a organização não sobrevive a um desastre natural. A disponibilização de soluções de recuperação de sistemas de informação deve ser flexível e economicamente viável para que a organização tenha a capacidade de recuperar rapidamente. A rápida recuperação das organizações face a desastres naturais, ou de uma falha de serviço, minimiza claramente as suas perdas que de outro modo seriam irrecuperáveis inviabilizando a continuidade dos seus serviços. Segundo Gallagher (2003), existem três soluções chave, ou elementos base, para as organizações considerarem quando se aborda o tema de continuidade de negócio, nomeadamente: antecipar incidentes (prevenção); saber que funções afetar e a que processos críticos; planear soluções testando previamente a resposta a qualquer incidente. Um plano de continuidade de negocio é essencial para a salvaguarda das organizações mediante desastres imprevistos e deverá incluir um plano de recuperação de desastres (PRD), composto principalmente pelos seguintes elementos: plano de resposta de emergência que salvaguarda pessoas e bens numa fase inicial; plano de gestão de crise que deve ser controlado por uma equipa previamente formada para o efeito que deve conduzir o comportamento da organização ao longo do período de crise; o plano de recuperação tecnológica para os sistemas de tecnologias de informação (TI) que sustentam e suportam o negócio da organização; plano de processos alternativos de negócio vai permitir a continuidade das operações mínimas da organização, ao longo do período de crise, evitando que a organização fique indefesa e não tenha qualquer capacidade de resposta neste período (Gallagher, 2003).

2.1.1 **Definições e Conceitos de Plano de Continuidade de Negócio**

Podemos definir o PCN, no seu aspeto mais simples, como um processo interativo que foi criado para identificar funções de negócio, tais como: críticas e políticas, processos, planos e procedimentos de modo a garantir a continuação das funções da organização no caso de um evento não previsto (Nickolett, 2001). Embora existam organizações similares dentro da mesma área de negócios, cada organização é única, assim como o seu funcionamento e as suas necessidades exigindo, também, a aplicação de um PCN específico, adequado à organização, em detrimento da aplicação de um PCN *standard* com um caminho simples e rápido que não promove a salvaguarda do funcionamento da organização. Um dos principais procedimentos a considerar no PCN é a análise e definição do que é ou não crítico dentro de uma organização,

para tal é necessário determinar as funções de negócio consideradas críticas e de extrema importância para a sobrevivência da empresa.

O Business Continuity Institute (BCI) define o PCN como um planeamento necessário que pretende antecipar um desastre, que pode afetar as funções da organização, para garantir que o plano responde a qualquer desastre do modo planeado e testado garantindo a manutenção da organização (Business Continuity Institute, 2011).

A Infosistema (Infosistema, 2010) define o PCN como um processo de Gestão essencial que tem como objetivo a manutenção e reposição dos processos de produção de negócio da organização incluindo pessoas e bens.

De forma geral, o PCN pode ser definido como um plano de resposta a uma emergência que garante a disponibilidade de recursos de sistemas críticos promovendo a recuperação da organização e ao seu normal funcionamento, este plano de resposta também incluí as operações de *backup* e recuperação de ativos atingidos por um desastre.

Segurança e Risco

A análise da segurança e do risco são dois conceitos inter-relacionados com o PCN e devem anteceder à implementação e execução de um plano de continuidade de negócio. A análise dos possíveis riscos deve ser realizada antes da elaboração de uma estratégia de continuidade. O objetivo de avaliar a segurança e o risco é reduzir, antecipar e gerir os riscos como rotina diária integrada na organização para auxiliar a tomada de decisões com base na análise dos resultados (CAVALCANTI, 2000 p.5).

Para realizar uma estratégia de continuidade de negócio é primeiramente realizada uma análise dos riscos (capítulo 2.3)

Impacto vs Probabilidade

Segundo Cavalcanti, (2009, p.25, apud Parreira & Lorga, 2013), tanto o impacto como a probabilidade devem ser definidos numa matriz com prioridades para as ações a corrigir nos sistemas e nos processos críticos de negócios na organização.

Prejuízo e o Impacto

Segundo Cavalcanti, (2009, p.25, apud Parreira & Lorga, 2013), o prejuízo e o impacto do mesmo geram custos sobre perdas de infraestruturas na organização que pode ficar impossibilitada de continuar a fornecer bens ou serviços prejudicando a continuidade do negócio. O impacto pode ter diferentes durações (curta, média ou a longo prazo) com

consequências diretas ou indiretas. As consequências diretas são referentes à perda da infraestrutura da arganização, ou seja, à construção do edifício, enquanto as indiretas são referentes à perda de informação necessária que impossibilita o funcionamento parcial ou total da organização continuar a executar as suas funções. A reflexão e análise do impacto quantifica, ou calcula, as consequências de ocorrer um desastre na organização (apud Parreira & Lorga, 2013).

O objetivo do **ponto de recuperação, ou *recovery point objective* (RPO)** está centrado nos dados e na flexibilidade de perda de dados da organização calculada num determinado tempo. O ponto de recuperação analisa o tempo entre a recuperação de dados, ou backups, e a sua relação com a quantidade de dados que podem ser perdidos entre os backups. Claramente como parte do plano de continuidade de negócios é necessário definir em quanto tempo é possível a organização recuperar ou tentar salvar o conteúdo perdido. O tempo no RPO deve ser o indicador das possibilidades de tolerância que a organização possuí para salvar os dados perdidos. A tecnologia que a organização utiliza para atualizar e recuperar os dados influência e pode diferenciar claramente o tempo do RPO de uma determinada organização. De modo sucinto RPO significa o tempo máximo durante o qual antes do desastre (tempo anterior, ou tempo para trás) os dados não foram salvos. Um exemplo de RPO é a previsão que uma organização tem de sobreviver entre três a quatro dias entre os backups, então o cálculo de tempo do RPO da organização é de três dias que é o intervalo de tempo menor entre a recuperação dos dados, ou backups. Outro exemplo, um RPO de 24 horas indica que o tempo máximo de dados perdidos é de 24 horas nas quais antes do desastre a organização não realizou backups sendo esse o ponto de recuperação. (posted in *Business*, *General Articles B* and tagged *2014 July14 BCP B*, *BCP*, *Business Continuity*, *QS 3*, *RPO*, *RTO*, *RTO and RPO defined*, *RTO vs RPO*, *What is RPO?*, *What is RTO?*.), (Heng, 2011).

O **objetivo de tempo de recuperação, ou recovery time objective (RTO)** tem como objetivo calcular a rapidez de tempo que a organização precisa para recuperar de um desastre e influência diretamente o orçamento geral que deve ser atribuído ao plano de continuidade de negócio, assim como os preparativos que devem ser implementados na organização. Por exemplo, uma organização que calcule que o seu RTO é de 3 horas, significa que a empresa consegue sobreviver durante este período de tempo, no entanto o nível de preparação desta empresa é elevado e os custos do orçamento são elevados garantido que os sistemas podem recuperar rapidamente. Outro exemplo é o de uma organização que prevê que o seu RTO é de

três semanas, o que significa que a empresa consegue sobreviver durante este período de tempo, no entanto o nível de preparação desta empresa é menos elevado e os custos do orçamento do PCN são mais baixos e o investimento é realizado em soluções menos avançadas (*posted in Business, General Articles B and tagged 2014 July14_BCP B, BCP, Business Continuity, QS 3, POR, RTO, RTO and POR defined, RTO vs RPO, what is POR?, What is RTO?.),* (Heng, 2011).

Tal como podemos observar na Figura 1 o tempo máximo tolerável de inatividade, *Maximum Tolerable Downtime* (MTD) ou Período Máximo de tempo tolerável (MTPD) antes da sobrevivência da organização estar em risco é um indicador do período de tempo máximo no qual uma organização pode estar inoperante. (ISO 22301: 2012 - Societal Segurança - Sistemas de Gestão de Continuidade de Negócios - Requisitos), (Heng, 2011).

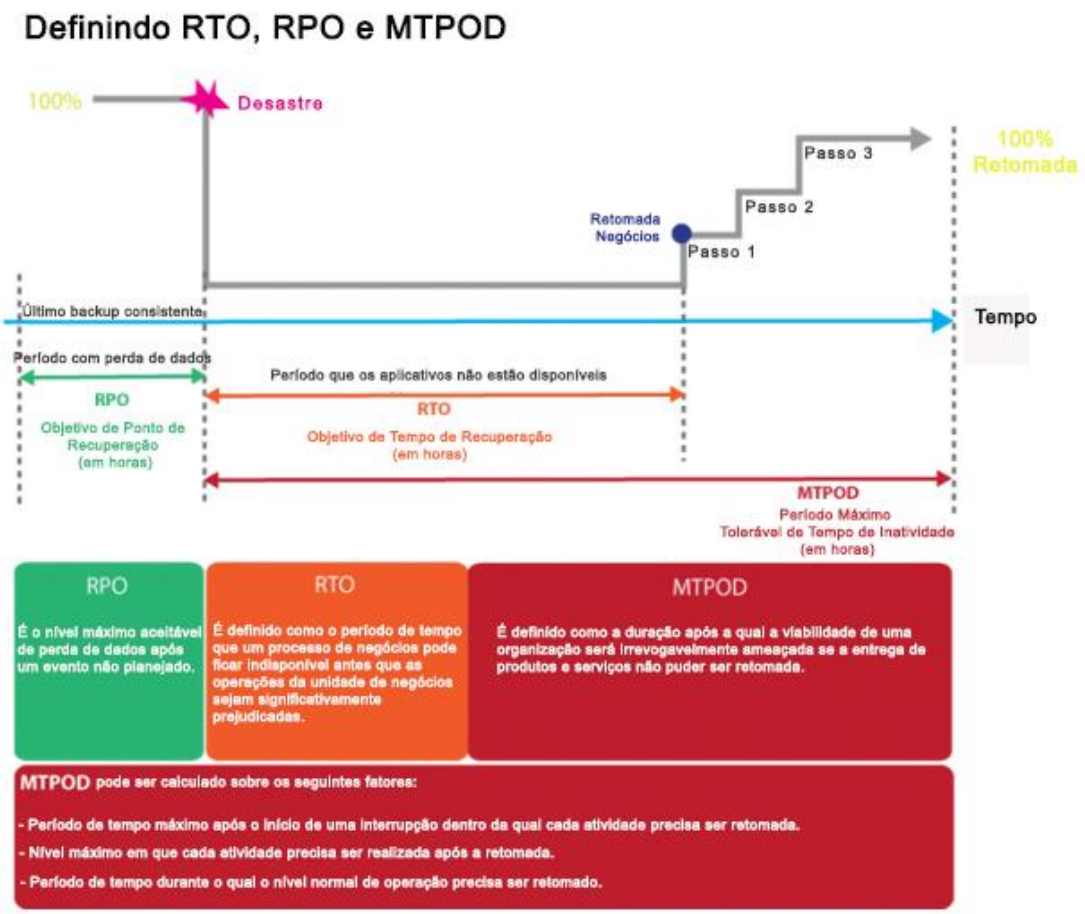


Figura 1: Definição de RTO, RPO e MTD

Fonte: (Adaptado de Heng, 2011)

2.1.2 **EVOLUÇÃO HISTÓRICA**

A atividade de continuidade do negócio é relativamente recente, ou seja, considerada ainda dentro do procedimento de gestão de riscos, esta surge, segundo a IBM (1999), como atividade comercial num processo formal nos anos 80 e servia particularmente para a proteção dos CPDs (Centrais de Processamento de Dados), que eram a base da estrutura de TI de uma organização. O processamento de dados, com um modelo que anteriormente era centralizado, sofreu alterações no início dos anos 90 e deu lugar ao modelo de processamento de dados distribuído e o surgimento da tecnologia cliente-servidor. O processamento de dados passou a ser claramente fundamental ao negócio de qualquer organização e as TI interligaram todos os segmentos da organização.

Com a era do computador começaram a surgir, por parte das organizações e dos seus responsáveis, preocupações pela proteção dos dados computacionais, com a segurança dos mesmos e com os mecanismos que de algum modo poderiam garantir e manter a continuidade do negócio ativo (Guindani, 2008).

Neste contexto são criadas iniciativas para manter a continuidade do negócio, nomeadamente: o planeamento dos recursos da empresa, a gestão de fornecedores e a gestão da relação com clientes. Atualmente, as organizações não conseguem ter o negócio ativo sem o recurso da TI (IBM, 1999).

O processo de continuidade de negócios teve uma evolução contínua e mantem um plano das atividades e dos recursos em constante atualização a par da evolução do negócio da organização. A evolução histórica da continuidade do negócio é representada na Figura 2 que se segue:

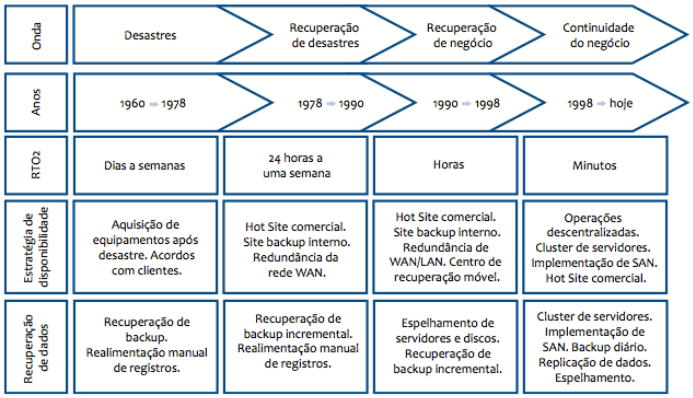


Figura 2: Evolução histórica da continuidade do negócio

Fonte: (Adaptado de Guindani, 2008)

Em 1980 a oferta de serviços na área de recuperação de dados aumenta, inclusive na recuperação de *"sites",* o que originou o crescimento de centros de recuperação cada vez mais aprimorados e com recursos cada vez mais sofisticados.

Em 1990 o Plano de Recuperação de Dados (PRD) passa para o BCP que dá origem a um sistema ainda mais complexo passando para o «Business Continuity Management» (BCM).

Existiram fatores considerados os impulsionadores da continuidade de negócio e da evolução histórica das TI. Claramente, em 2001 o BCM ocupa um espaço proeminente para os órgãos de gestão das organizações que compreendem que a sua sobrevivência depende da implementação deste plano para uma proteção eficaz dos seus dados.

Os dois principais fatores, já a seguir nomeados, foram considerados como impulsionadores da continuidade de negócio:

O Bug do milênio, com data e hora marcada para acontecer, foi considerado uma ameaça sem antecedentes na evolução histórica da TI. Neste contexto, específico, as avaliações deram lugar a indemnizações judiciais que atingiram valores de triliões de dólares, enquanto os bancos investiram para proteger os seus sistemas de dados, como por exemplo, o Citibank investiu milhões de dólares para adequar os seus sistemas de dados (GUINDANI, 2008).

O atentado terrorista do onze de setembro de 2001 fez desaparecer um símbolo de poder dos EUA quando desabaram as torres gêmeas. A partir deste acontecimento as empresas conseguiram observar a sua vulnerabilidade a eventos que podem ameaçar os seus negócios. Neste contexto, as organizações perceberam que a realização de uma avaliação de risco, mesmo sendo bem planeada, não garante a segurança dos seus negócios e a ocorrência de desastres catastróficos, mas pode reduzir os seus impactos com a implementação da BCM.

2.1.3 **Elementos Fundamentais para um Plano de Recuperação de Desastres**

Tal como é referido na revista COMPUTERWORLD de 28 de fevereiro de 2011 no Dossier: *Disaster Recovery* sobre a gestão de continuidade de negócios (BCM) e o plano de recuperação de desastres existem alguns elementos fundamentais a considerar quando é realizado um plano desta natureza, nomeadamente os seguintes elementos:

- Os órgãos de decisão devem definir uma equipa responsável pelo departamento de Plano de Continuidade de negócio e recuperação de desastres;

- Definir o plano adequado à realidade e ao contexto da organização;

- Justificar o plano e identificar os erros de maior importância;

- Realizar testes no contexto da vida real da organização;

- Entender o negócio e o contexto onde se desenvolve o mesmo na organização;

- Identificar os custos de indisponibilidade e as verbas disponíveis;

- Retirar e armazenar os dados das instalações;

- Além da simples recuperação é necessária a realização da gestão do armazenamento;

- Adotar um conjunto de estratégias de tolerância ao desastre para aplicações e dados como '*wide area' clusters*, replicação de armazenamento e replicação de aplicações entre outras";

- Utilizar a suporte *backup* e para além deste suporte pensar na possibilidade de aquisição de uma *Storage Área Network* (SAN) com um sistema de backup num centro de dados remoto;

- Melhorar o plano de negócio com soluções de armazenamento virtual em nuvem, (*Cloud).*

2.1.4 **Esquema da Estrutura Metodológica para Elaborar um Plano de Continuidade de Negócio**

Segundo Heng (2014) a maioria dos padrões de um Plano de Continuidade de Negócio são semelhantes, exceto no modo como são escritos que tendem a parecer diferentes uns dos outros, no entanto, o conteúdo é geralmente semelhante e a abordagem pode ser comum sem que a organização necessite de realizar grandes mudanças no programa de Continuidade de Negócio da organização. Para tal, devem ser considerados os pontos-chave comuns independentemente do padrão do Plano de Continuidade de Negócio internacional ou nacional adotado, a organização deve ser capaz de adotar uma abordagem comum. Claramente que a utilização da Metodologia de Planeamento do PCN é o ponto-chave para uma abordagem comum dentro da organização.

No documento de requisitos ISO 22301 o elemento do programa de Continuidade de Negócio é realçado como um componente cujos detalhes estão claramente destacados como o elemento do programa de Continuidade de Negócio na norma ISO 22301 (orientação).

O gráfico da Figura 3, ilustra a comparação do planeamento do PCN (linha superior de cor azul) com a estrutura metodológica dos elementos do programa de Continuidade de Negócio conforme especificado na ISO 22301 (coluna esquerda com a cor vermelha).

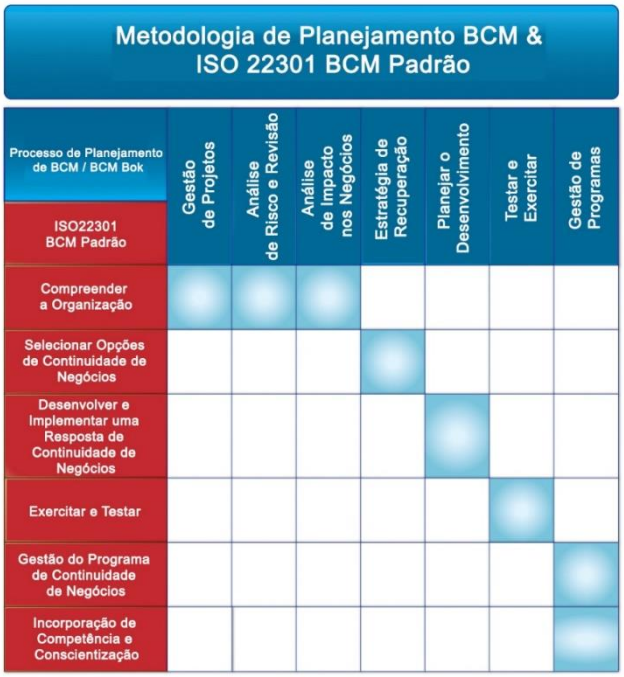


Figura 3: Comparação da Metodologia de Planeamento BCM com os Elementos ISO 22301 do Programa BC **Fonte:** (Adaptado de Heng, 2014)

O gráfico apresentado ajuda os profissionais a perceber o planeamento formal dos elementos ISO 22301.

Segundo Heng (2013), conclui-se, tal como se pode observar na Figura 4, que os requisitos da documentação ISO 22301 estão no cerne de qualquer sistema de gerenciamento de continuidade de negócios da ISO 22301 (BCMS).

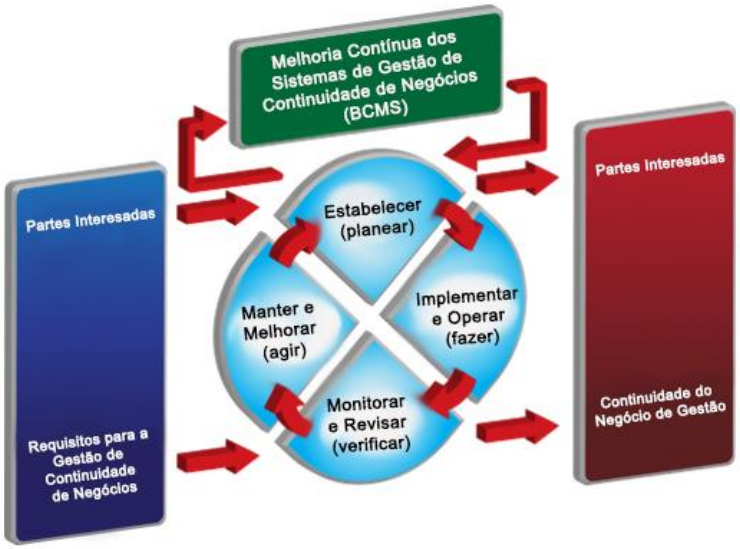


Figura 4: PCDA Cycle Applied to BCMS Processes

Fonte: (Adaptado de Heng, 2013)

Há dois aspetos importantes que as organizações devem realizar, nomeadamente:

(1) Documentar toda a ISO 22301 BCMS (a norma ISO 22301: 2012 contém requisitos precisos para os vários documentos);

(2) A organização deve seguir todo o processo que está contido na documentação ISO 22301. É importante notar que a organização não só precisa de ter um conjunto de documentos ISO 22301, mas também precisa realmente conduzir as suas práticas de continuidade de negócios de acordo com esses documentos. A documentação ISO 22301 é eficiente e não aumenta a burocracia na organização, define onde é necessário calibrar entre o que é um bom BCM e o que é uma boa ISO BCMS documentação.

Segundo a *University of Toronto Information* (University of Toronto Information, 2012) a metodologia utilizada para o desenvolvimento dos planos deve considerar os seguintes pontos-chave:

- Os órgãos de gestão da organização devem ter uma visão abrangente do esforço total necessário para compreender e desenvolver um plano de recuperação eficiente;
- Os órgãos de gestão devem estar de acordo e estabelecer um compromisso que transmita o esforço total necessário participando nesse esforço;
- Partindo da análise das funções de negócio é necessário definir requisitos e condições de recuperação;
- Justificar, através de documentação, qual o impacto de uma perda caso a mesma atinja as funções chave de negócio na organização;
- Manter a atenção constante na prevenção de desastres e na minimização de impacto para manter uma recuperação organizada numa planificação;
- Selecionar e manter uma equipa de projeto para garantir o equilíbrio do plano ao longo do seu desenvolvimento;
- Desenvolver um plano de contingência claro, simples de utilizar e simples de manter perante situações imprevisíveis;
- Integrar na planificação da organização os negócios em desenvolvimento e os processos de desenvolvimento de sistema.

2.1.5 **Abordagem às Fases do Projeto de Gestão de Continuidade de Negócio**

Segundo a Sonaecom (2008), a abordagem metodológica das fases do projeto de gestão de continuidade de negócio envolve as 5 fases que se seguem:

Fase 1: Representa a compreensão do negócio com uma análise de impacto de negócio, uma avaliação de riscos e uma definição abrangente de BCM.

Fase 2: Representa a definição de estratégias BCM com uma identificação que carateriza a estratégia de recuperação, com uma definição de medidas de gestão do risco e uma análise de vantagens e desvantagens nomeada em cada uma das estratégias.

Fase 3: Representa o desenvolvimento e implementação do plano BCM através de um plano de gestão de crise corporativo, um plano de continuidade de negócio e o desenvolvimento e implementação sustentados por soluções de Continuidade.

Fase 4: Representa a manutenção de planos atualizados, os testes e simulação dos planos e a auditoria aos processos BCM (Sonaecom, 2008).

A Figura 5 resume as diferentes fases de continuidade de negócios da seguinte forma:

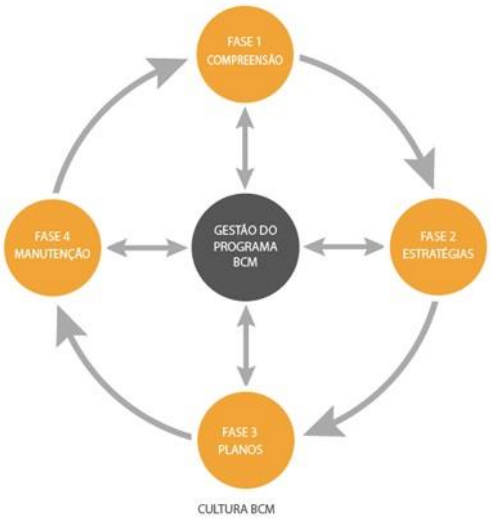


Figura 5: Abordagem à Gestão de Continuidade de Negócio

Fonte: (Adaptado de Sonaecom, 2008)

Na última fase, no centro da Figura 5, existe a divulgação da gestão do programa BCM na organização através da divulgação e formação dos colaboradores, implementação da cultura BCM comum a todos os elementos dentro da organização finalizando com a monotorização da mudança. Para que a implementação de um projeto com estas carateristicas seja realizado com sucesso é importante "...embeber a cultura BCM na organização…" (Sonaecom, 2009).

Tal como se pode observar na Figura 6, quando uma organização projeta um Plano de Continuidade de Negócio deve considerar as seguintes etapas no processo:

- Confirmação da necessidade de organizar o plano;
- Definir uma equipa específica para colocar em prática o plano;
- Planificar e definir planos alternativos para ameaças eventuais de desastres;
- Escrever o plano de recuperação de ameaças e desastres e continuidade de negócio;
- Testar os ensaios do plano de recuperação de desastres e continuidade de negócios;

- Manter e atualizar o plano de recuperação de desastres e continuidade de negócio;
- Implementar e avaliar continuamente o plano de recuperação de desastre e continuidade de negócio.

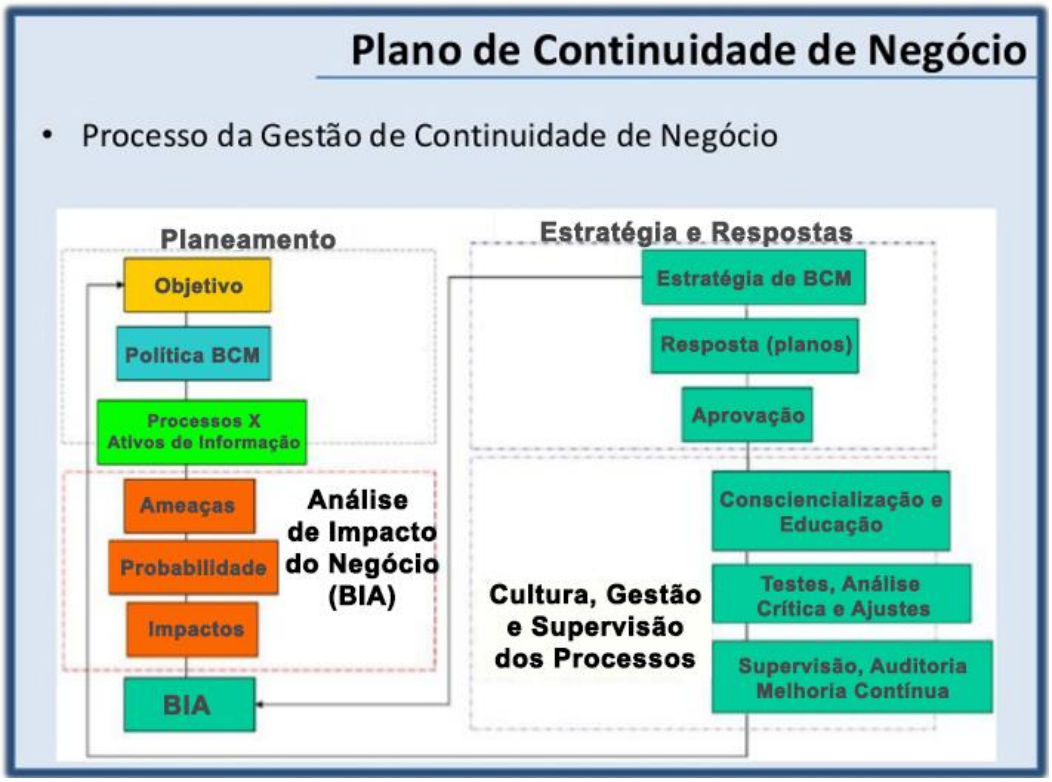


Figura 6: Processo das Atividades Principais do Plano

Fonte: (Adaptado de Infosistema, 2010)

2.1.5.1 **Identificação de Riscos e Análise de Impacto**

Tal como se pode observar na Figura 7, existe a necessidade de realizar uma análise dos riscos para determinar quais são as funções afetadas pelos impactos e planificar uma estratégia. (Trindade, 2008) A análise de riscos permite identificar a origem dos riscos e posteriormente através da análise BIA é possível identificar a origem dos mesmos. Desse modo é possível identificar através da análise BIA as funções críticas do negócio e detetar a sua hierarquia.

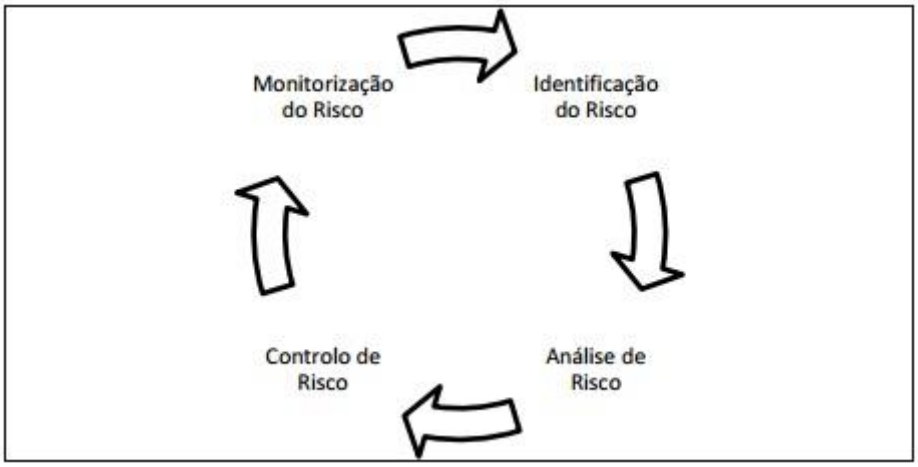


Figura 7: Ciclo de Gestão de Risco

Fonte: (Gallagher, 2003, p. 9)

A análise de risco serve para obter uma relação dos ativos críticos para determinar os riscos e a vulnerabilidade associada a esse risco. A análise em questão tem os seguintes benefícios instantâneos: permite o conhecimento real da situação da organização, a identificação das medidas de segurança corretas e adaptadas ao problema, a melhor aplicação de recursos e a possibilidade de tomar decisões apoiadas em fatores reais.

Tal como mostra na Figura 8 vamos passar a descrever as três faces do quadrado sobre a análise de risco dos processos de SI e TI:

- **Ambiente interno:** aborda aspetos da culturais da organização;
- **Definição de objetivos:** caraterizados pelas metas estratégicas definidas pela organização;
- **Identificação do evento:** identifica os eventos internos e externos que podem influenciar o cumprimento dos objetivos estratégicos;
- **Avaliação do risco:** análise quanto à probabilidade e o impacto dos riscos, de modo a determinar formas de gestão dos mesmos;

- **Resposta ao risco:** delinear medidas para salvaguardar, aceitar, reduzir ou transferir riscos;
- **Atividades de controlo:** definir e implementar políticas e procedimentos que possam assegurar resposta aos riscos identificados;
- **Informação à comunicação:** identificar e recolher informação para responder às responsabilidades no cumprimento da gestão de riscos;
- **Supervisão:** supervisionar as políticas e procedimentos através de avaliações periódicas e auditorias.

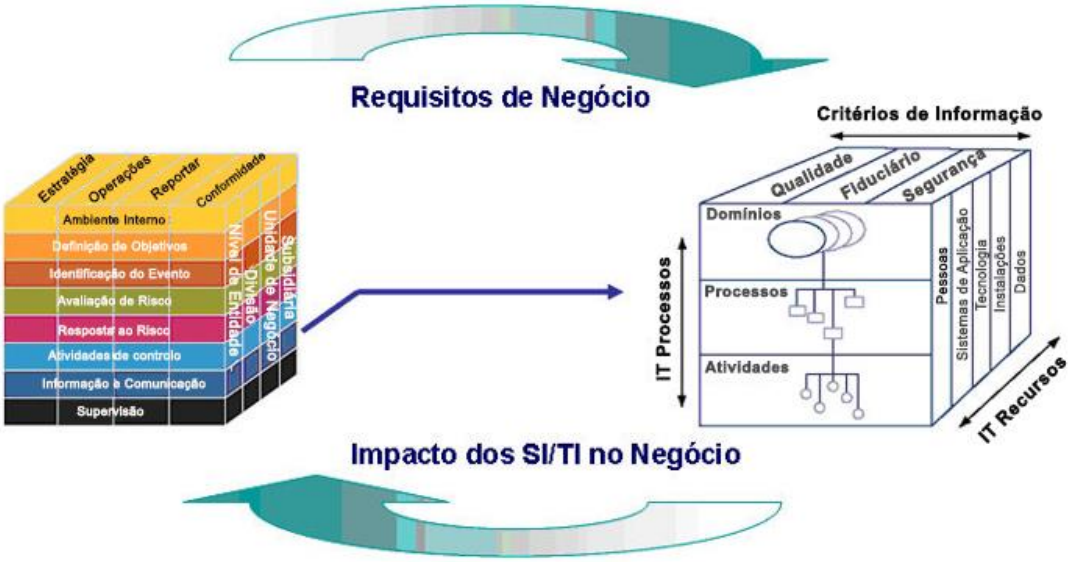


Figura 8: Análise de risco dos processos de SI e TI

Fonte: (Adaptado de Sinfic SA.)

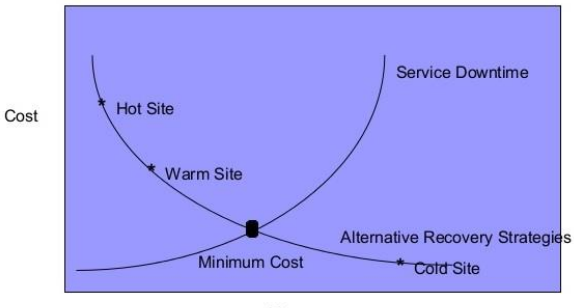
2.1.5.2 **Estratégias para Recuperação de TI**

É necessário descrever uma estratégia para identificar medidas eficazes na gestão de continuidade de negócio através dos *inputs* da análise de risco BIA. Por meio destas medidas, perante uma avaliação de custo e benefício, é possível tomar decisões que determinam o tempo de recuperação de cada uma das funções críticas da organização. Nesta fase também se procede à definição da abordagem para recuperação das SI/TI. Tal como se observa na Figura 9, considerando a existência de vários tipos de estratégia de recuperação de TI, pode-se descrever, as mesmas, da seguinte forma:

- *Hot-site* – Instalação de um centro de dados com hardware disponível para favorecer interfaces de comunicação e espaço num ambiente controlado com capacidade de fornecer um sistema de backup contínuo e imediato de apoio ao processamento de dados. Esta instalação permite, em caso de indisponibilidade do centro de processamento de dados principal, que o utilizador do sistema não tenha perceção da quebra do serviço devido a existirem dois centros de processamento de dados.

- *Warm-site* – Os aplicativos trabalham com um ou dois centros de processamento de dados e são necessárias aplicações. É aplicado a sistemas com tolerância superior à paragem ou quebra do serviço, a indisponibilidade pode prolongar-se por um período maior até voltar a estar operacional, sem comprometer o serviço ou a ocorrência de gerar impactos consideráveis.

- Cold-site – A partir de um ambiente com o mínimo de recursos ao nível das infraestruturas e telecomunicações, esta proposta é uma alternativa clara de contingência. Aplica-se unicamente em situações de grande intolerância à indisponibilidade. A reinstalação de todo o sistema é necessária para restabelecer os aplicativos, neste caso, o centro de processamento de dados secundários serve apenas a infraestrutura de comunicação (Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R., 2002).



Site	Custo	*«Hardware»*	Comunicações	Tempo de instalação	Localização
Cold Site	Baixo	Nenhum	Nenhum	Elevado	Fixo
Warm Site	Médio	Parcial	Parcial/Total	Médio	Fixo
Hot Site	Médio/alto	Total	Total	Curto	Fixo

Figura 9: Custos de Rutura em contraste recuperação para selecionar critérios de site alternativo **Fonte:** (Adaptado de Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002)

2.1.5.3 **Fase de Implementação**

Após a fase anterior sobre as estratégias, a fase de implementação é descrita visualmente através da Figura 10. Após cada um dos elementos da equipa estarem identificados devem ser escritos vários Planos de Continuidade de Negócio, tais como:

1) Plano de Resposta de Emergência: descreve o que deve ser realizado após o incidente e quem são os decisores nesta fase;
2) Plano para reaver as operações de Negócio: descreve como devem ser reativadas as funções críticas de negócio;
3) Plano de recuperação do incidente ou fase de retorno: descreve como recuperar as instalações técnicas e administrativas (Cornish, 2001).

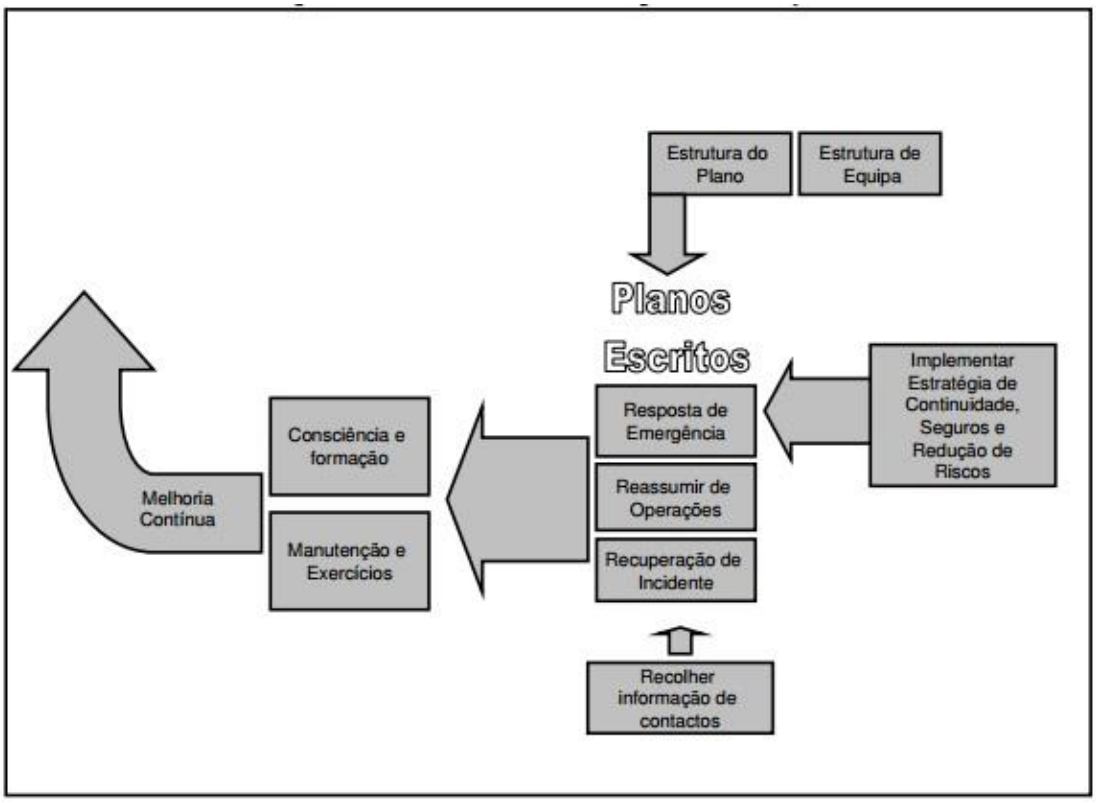


Figura 10: Fase de Implementação

Fonte: (Trindade, 2008)

2.1.5.4 **Fase de Gestão**

A fase de gestão é essencial para manter o Plano de Continuidade ativo e atualizado.

É importante definir quem é o principal responsável por verificar e manter o plano com verificações periódicas atualizado. Por norma, o responsável pela gestão representa a designação de coordenador do Plano de Continuidade de Negócio (Cornish, 2001).

O coordenador do Plano deve comprometer a gestão de topo no acompanhamento e patrocínio da Gestão e Manutenção do PCN.

2.1.5.5 **Fases de Recuperação definidas pelo PCN**

Outra cronologia importante é a que resulta como *output* do projeto e que estabelece as fases do processo de Recuperação em caso de desastre, tal como podemos analisar na Figura 11.

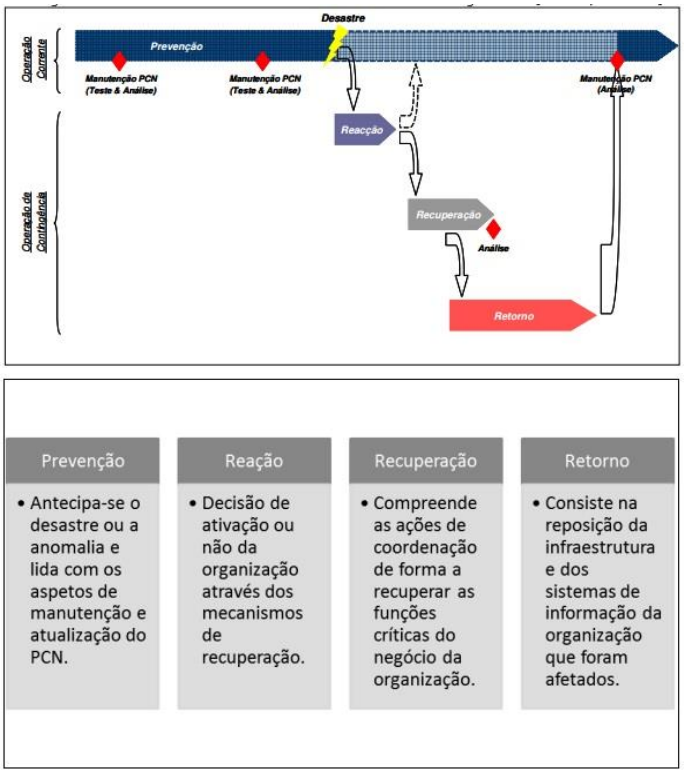


Figura 11: Fases de Recuperação definidas pelo Plano de Continuidade Negócio

Fonte: (SIBS, 2006)

2.1.6 **Benefícios da Continuidade de Negócio**

O plano de recuperação de desastre e continuidade de negócio tem alguns benefícios associados de diversas origens, tais como:

- Económica;
- Informática;
- Humana;
- Funcional.

Estes benefícios podem ser analisados a diferentes níveis, cada um dos benefícios está ligado a uma camada da hierarquia das organizações, tal como:

- **Operacional** – aumenta a eficiência nas operações e processos da organização e melhora a imagem que os clientes têm sobre o serviço;
- **Tático –** trazem vantagens às camadas intermédias de Gestão, tais como: melhores sistemas de informação que possibilitam a tomada de decisões de modo mais rápido e preciso.
- **Estratégico** – diretamente relacionados com a implementação da estratégia da empresa, como por exemplo: na aquisição de vantagens competitivas sobre os concorrentes;
- **Organizacionais** – não têm valor direto, tanto para as operações como para a gestão ou estratégia (Ezingeard et al, 2005). Nos benefícios organizacionais incluem-se os benefícios de cumprimento de regulamentações do setor.
- **Económicas**;
- **Legais**.

2.2 **GESTÃO DE RISCO**

Considerando que existem cada vez mais variáveis, tais como: a globalização, a complexidade dos produtos e serviços, a nova era digital, as leis reguladoras e o mercado, segundo diferentes autores a gestão de risco é cada vez mais um fator decisivo na estratégia das organizações (The Institute of Risk Management et al., 2002; Cavalcanti, 2009).

Segundo Gonçalves (2011) é fundamental para a gestão, existir um equilíbrio entre o investimento controlado e o nível de risco, os custos financeiros devem estar em sintonia com o nível de risco e a tolerância a esse risco para evitar custos dispensáveis. Gonçalves indica que a avaliação de riscos possibilita a Gestão de Topo tomar decisões sobre os investimentos controlados no nível de risco aceitável para a Organização, perante os riscos nos quais a empresa está exposta.

Silva & Torres (2010), consideram a gestão de risco um mecanismo fundamental para planear qualquer atividade e sem este mecanismo podem ocorrer, de modo inexplicável, erros de planeamento. Silva et al. (2010) indica que a gestão de risco deve estar presente em todas as fases de um projeto, como um ciclo que permite identificar as ameaças, a qualificação do risco, a redução do risco residual e a sua aceitação residual.

Segundo Cavalcanti (2009), "(…) gerir riscos tornou-se fundamental para tratar lacunas de controlo e principalmente, fornecer uma visão macro da organização (…)". A Norma de Gestão de Riscos define a gestão de riscos como "(…) o processo através do qual as organizações analisam metodicamente os riscos inerentes às respetivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades."

Tal como podemos observar na Figura 12, na medição das consequências perante as ameaças, ao longo do processo de gestão de risco está intrínseca a seguinte sequência de etapas:

- A identificação dos riscos é necessária para a análise quantitativa do risco. Este risco é medido pelo impacto que resulta da materialização da ameaça;
- A identificação das ameaças através da preparação de cenários que facilitam a aquisição de informação estatística sobre a frequência das ocorrências passadas que servirão para quantificar os riscos nos próximos passos da organização;
- A identificação das vulnerabilidades permite calcular as probabilidades de materialização das ameaças na organização;
- A análise quantitativa, quantifica e qualifica, os danos gerados pela probabilidade das ameaças numa análise de riscos.

Nível de Impacto	Descrição do Impacto
Alta	O impacto financeiro sobre a organização deve ultrapassar os X€ Impacto significativo sobre a estratégia ou atividades operacionais da organização Grande preocupação dos intervenientes.
Média	O impacto financeiro sobre a organização deve ser entre X€ e Y€ Impacto moderado sobre a estratégia ou atividades operacionais da organização Preocupação moderada dos intervenientes.
Baixa	O impacto financeiro sobre a organização deve ser inferior a Y€ Impacto baixo sobre a estratégia ou atividades operacionais da organização Pouca Preocupação dos intervenientes.

Figura 12: Avaliação das consequências perante as ameaças

Fonte: (UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management, 2002, p. 8)

A definição de risco é qualquer situação que pode afetar a capacidade da organização alcançar objetivos e está relacionada a qualquer decisão das organizações. Tal como refere Cavalcanti (2009), o risco é a "(…) ameaça de que um evento ou ação (interno ou externo) possa afetar negativa ou positivamente o ambiente no qual se está inserido". Também podemos descrever o risco como "(…) a combinação da probabilidade de um acontecimento e das suas consequências" (A Risk Management Standard, 2002, p. 3).

Gonçalves (2011) considera o risco evitável e por esse motivo a organização deve optar por tratar de analisar o risco.

Outros autores defendem que os gestores compreendem a gestão de risco como a origem de oportunidades que diferenciam a organização devido a criarem sobre os eventos incertos formas preventivas de o tratarem criando oportunidades de lucro, enquanto outros gestores consideram a gestão de risco como um mal necessário (Cavalcanti, 2009) (Gonçalves, 2011). Gonçalves (2011) também indica que as organizações devem cultivar uma cultura que favoreça a gestão de risco que deve partir da Gestão de Topo e expandir-se por toda a organização, através da motivação no envolvimento dos funcionários nessa cultura da organização.

Interessa referir as caraterísticas especificas, da gestão de risco, em função do setor de atividade da organização. Nesta dissertação a gestão de risco está enquadrada nos riscos dos sistemas de

informação e tecnologias de informação. Os sistemas de informação e tecnologias de informação devem impedir o risco através dos acessos não autorizados para assegurar os dados e garantir a continuidade de negócio, caso ocorra uma falha.

Segundo o "Modelo de Avaliação de Risco (MAR)", referido por Gonçalves (2011) indica, relativamente aos riscos de sistemas de informação, a existência de cinco modos de classificação do risco:

- Risco de Estratégia – resultante dos riscos ligados a estratégias e políticas inapropriadas, definidas pela organização;
- Risco de Flexibilidade – resultante de riscos ligados a sistemas de informação complexos e sem flexibilidade;
- Riscos de Acesso - resultante dos riscos ligados a acessos não autorizados;
- Riscos de Integridade – resultantes dos riscos ligados à qualidade da informação gerada pelo sistema de informação;
- Risco de Continuidade – resultantes dos riscos ligados a falhas operacionais.

Podemos concluir que a gestão de risco é um processo de identificação e avaliação do risco, um meio para dar início a medidas preventivas para redução do risco de modo aceitável. O objetivo principal da gestão de risco é defender a organização e a sua aptidão para realizar a sua missão, pois permite aos gestores tomarem decisões com base na informação justificada de custos do orçamento estimado pelo TI. Dentro da organização a gestão de risco é uma função essencial para a proteção na gestão da organização.

2.2.1 **Os Benefícios da Gestão de Risco**

Segundo Cavalcanti (2009), após a implementação integrada na organização da gestão de riscos, refere os seguintes benefícios ou vantagens:

- Possibilita a organização a adquiri uma visão integrada dos processos de negócio;
- Possibilita os gestores a adquirem as melhores ferramentas de controlo perante a incerteza do contexto da organização;

- Possibilita determinar, perante os riscos, a possibilidade de perda de informação;
- Possibilita identificar situações de recuperação de dados;
- Possibilita eliminar fontes de risco e revertê-las em oportunidades;
- Possibilita uma garantia da continuidade de negócio;
- Possibilita a estrutura de uma cadeia de valor no mercado (condições internas e externas) no qual a organização está inserida;
- Possibilita a análise e a organização que permite interpretar os possíveis aspetos positivos e negativos de todos os agentes que podem afetar a organização;
- Possibilita a organização de atingir todos os objetivos globais e reduz a incerteza;
- Possibilita o sucesso através da redução do insucesso na organização.

2.2.2 **O Dicionário de Riscos**

Com uma função de catálogo, o dicionário de riscos contém as origens possíveis e individuais de risco relativamente a cada segmento do negócio da organização. A função deste dicionário é de fornecer o direcionamento das ações de gestão de risco e processos incluídos na cadeia de valor do negócio[1] da organização, assim como, as condições internas e externas de negócio (Cavalcanti, 2009). A Figura 13 permite a observação sumária da avaliação da cadeia de valor de riscos e processos.

[1] "A cadeia de valor designa uma série de atividades relacionadas e desenvolvidas pela empresa a fim de satisfazer as necessidades dos clientes, desde as relações com os fornecedores e ciclos de produção e venda até a fase da distribuição para o consumidor final (...)" Moura, 2006 (Cavalcanti, 2009, p. 10).

Figura 13: Avaliação da Cadeia de valor de riscos e processos

Fonte: (Cavalcanti, 2009, p. 10)

2.2.3 **Metodologia de Gestão de Risco**

Após a revisão das diversas normas para gestão de riscos, foi considerado o *Risk Management Guide for Information Technology Systems* (Stoneburner, Goguen, & Feringa, 2002) o sistema mais significativo para a investigação do presente trabalho, visto que a sua metodologia de gestão de risco abrange todas as fases do ciclo de vida de desenvolvimento de sistema.

Tal como já foi referido anteriormente, a gestão de risco é um processo que deve ser integrado na totalidade no SDLC e é aplicada do mesmo modo no SDLC, independentemente da fase SDLC que o processo de encontra. Stoneburner et al. (2002, p. 4) carateriza o SDLC como um sistema com cinco fases diferentes, nomeadamente:

1. Fase Inicial – A identificação dos riscos é utilizada para apoiar o desenvolvimento de requisitos de sistema, abrangendo as estratégias e os requisitos de segurança.
2. Fase de Desenvolvimento – A identificação dos riscos é utilizada para apoiar as análises de segurança do sistema que podem trazer alterações ao desenho e arquitetura ao longo do desenvolvimento do sistema.
3. Fase de Implementação ou codificação – Esta fase permite prestar suporte à avaliação da implementação do sistema em conformidade com as suas necessidades no seu ambiente operacional modelado.
4. Fase de Manutenção ou Operação – Anteriormente a esta fase, devem estar identificados todos os riscos. As atividades de manutenção devem ser realizadas de modo periódico, ou sempre que necessário quando sucedem mudanças significativas no ambiente operacional, ou seja, no ambiente de produção do sistema.
5. Fase de Eliminação – Esta fase é efetuada para componentes de *hardware* e *Software* do sistema no qual vão ser eliminados *ou* substituídos para garantir que são eliminados corretamente, para garantir que qualquer dado excedente tem um tratamento adequado de modo a diminuir ou eliminar qualquer risco.

Segundo refere Stoneburner et al. (2002, p. 4), a avaliação de risco é a primeira fase da proposta metodológica de gestão de risco. Esta primeira fase de avaliação de risco determina o grau de ameaça e o risco relacionado com o sistema de TI ao longo de todo o processo de SDLC. Desta análise resulta o relatório que identifica prováveis controlos que reduzem ou eliminam o risco. Tal como mostra a Figura 14 a avaliação de risco calcula a existência de 9 atividades.

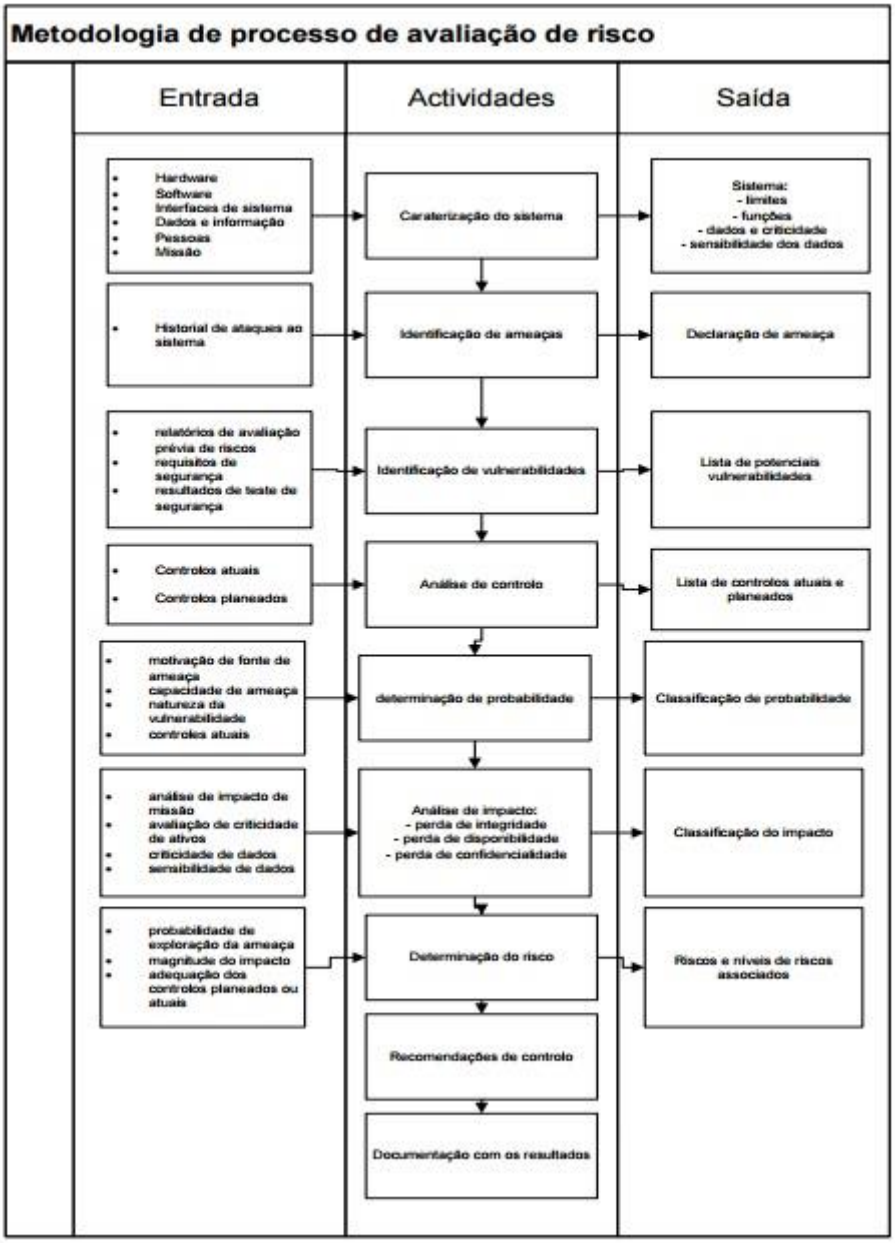


Figura 14: Metodologia de processo de avaliação de risco

Fonte: (Adaptado de Stoneburner, Goguen, & Feringa, 2002)

Na primeira atividade é caraterizado o sistema que prevê a definição do circuito do esforço de avaliação de risco, circunscrevendo os limites operacionais de autorização e dando informações essenciais para definir o risco sobre: o hardware, o software, os dados e informação, as interfaces de conetividade de sistema externas e internas, o pessoal responsável da divisão ou suporte, a missão do sistema, o valor que o sistema tem na organização, o nível de segurança exigido para manter a integridade confidencialidade e disponibilidade do sistema, as condições funcionais do sistema, as politicas de segurança, a arquitetura de sistema, a topologia de rede,

as informações sobre as politicas de armazenamento para segurança e proteção da sua confidencialidade, a integridade e disponibilidade de dados e sistemas, a segurança do ambiente físico.

Na segunda atividade é realizada a identificação de ameaças. Segundo refere João Luiz Pereira Marciano (2006) sobre o conceito de ameaça[2] nas suas pesquisas é praticável classificar as ameaças, tal como indica a Figura 15 e a seguinte lista:

1 – Possibilidades de ocorrência de ameaças através de fenómenos naturais ou ameaças naturais, tais como: terramotos, tornados, avalanches, tempestades, deslizamento de terra, inundações entre outros fenómenos naturais possíveis.
2 – Possibilidades de ocorrência de ameaças através de ameaças humanas, tais como: Ocorrências intencionais executados com a utilização do *software*; lapsos ou falhas técnicas de *software* (*bug*, falhas de codificação); erros humanos tais como acidentes, erros dos funcionários; ações intencionais de invasão, espionagem ou *hacking*; atos intencionais de sabotagem ou destruição de sistemas da informação; ações intencionais de roubo; ações intencionais de roubo de informação.
3 – Possibilidades de ocorrência de ameaças através de ameaças de ambiente, tais como: falha energética de longa duração; poluição; enganos ou falhas técnicas de *hardware*; outras ameaças de ambiente que possam existir.

Naturais	Incêndio
	Inundação
	Terramoto
Humanas	Erro de Operação
	Terrorismo
	Vírus
Equipamento	*Hardware*
	Software

Figura 15: Causas que implicam a ativação do Plano de Continuidade de Negócio

Fonte: (Adaptado de Jackson, 2007)

[2] Incidente ou postura indesejável que remove ou destrói um recurso informático e as informações com ele relacionadas.

Na segunda atividade é realizada a identificação de vulnerabilidades. Podemos definir vulnerabilidade como uma debilitação ou deficiência que possibilita a que ocorra uma determinada ameaça, tal como podemos observar na Figura 16, ou seja, é caraterizada como um sinal potencial de falha ou um componente relacionado com a informação que possibilita a sua observação por uma determinada ameaça. Podem ser utilizadas ferramentas tais como listas de verificação e ferramentas de *software* para identificar e determinar as vulnerabilidades, tal como indicamos na Figura 17 na lista verificação de critérios de segurança para identificar vulnerabilidades.

Probabilidade de ocorrência de ameaças		
Nível de Ameaça	Probabilidade de ocorrência	Indicadores
Alta	Com possibilidade de ocorrência todos os anos ou hipótese de ocorrência superior a 25%.	Potencial para ocorrer diversas vezes dentro do período de tempo (por exemplo – dez anos). Ocorreu recentemente.
Média	Com possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 25%.	Pode ocorrer mais do que uma vez dentro do período de tempo (por exemplo – dez anos). Pode ser difícil de controlar devido a algumas influências externas. Existe um historial de ocorrências.
Baixa	Sem possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 2%.	Não ocorreu. Improvável que ocorra.

Figura 16: Possibilidades de ocorrência de ameaças

Fonte: (UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management, 2002, p. 8)

Área	Critérios de segurança
Gestão de segurança	• Atribuição de responsabilidades; • Continuidade do apoio; • Capacidade de resposta a incidente; • Revisão periódica dos controlos de segurança; • Autorização de pessoal; • Avaliação de risco; • Segurança e formação técnica; • Separação de funções; • Sistema de autorização e reautorização; • Sistema ou plano de segurança de aplicações.
Segurança operacional	• Controlo de contaminantes pelo ar (fumo, poeira, substâncias químicas); • Controlos para assegurar a qualidade da fonte de energia elétrica fonte; • Acesso e eliminação de dados; • Distribuição de dados externos e rotulagem; • Proteção das instalações; • Controlo de humidade; • Controlo de temperatura; • Postos de trabalho, portáteis, etc.
Segurança técnica	• Comunicações (*routers*, *firewall*, etc.); • Encriptação; • Controlo de acesso discricional; • Identificação e autenticação; • Deteção de intrusão; • Auditoria do sistema;

Figura 17: Lista verificação de critérios de segurança para identificar vulnerabilidades

Fonte: (Adaptado de Stoneburner, Goguen, & Feringa, 2002)

Tal como indicam Stoneburner et al. (2002), na quarta atividade é necessária a análise de controlos que foram executados ou estão planificados para execução, pela estrutura da organização, para reduzir ou eliminar a probabilidade de uma ameaça exercer uma

vulnerabilidade no sistema. Stoneburner et al. (2002), indicam que na quinta atividade o objetivo é a aquisição de uma classificação geral de probabilidades que indica o potencial de uma vulnerabilidade, esta pode ser praticada na classificação de um determinado ambiente de ameaça, considerando os seguintes fundamentos para a sua ocorrência:

- Aptidão e motivação da origem, ou fonte, da ameaça;
- Essência da vulnerabilidade;
- Presença e eficácia dos controlos presentes atualmente;

Podemos observar na Figura 18 as definições de probabilidade de uma potencial vulnerabilidade caraterizada como: alta, média ou baixa.

Nível	Definições de probabilidade
Alta	A fonte de ameaça é suficientemente capaz e altamente motivada, e os controlos para evitar a vulnerabilidade são ineficazes.
Média	A fonte de ameaça é motivada e capaz, mas controlos implementados são capazes de impedir o exercício bem-sucedido da vulnerabilidade.
Baixa	A fonte de ameaça não tem motivação ou capacidade, ou existem controlos para impedir, ou pelo menos dificultar significativamente a vulnerabilidade de ser exercida.

Figura 18: Classificação geral de probabilidade de uma potencial vulnerabilidade

Fonte: (Adaptado de Stoneburner, Goguen, & Feringa, 2002)

Segundo Stoneburner, Goguen, & Feringa, (2002), a sexta atividade é a análise de impacto (BIA)[3]. A análise desta atividade possibilita determinar os resultados hostis que resultam da prática de uma vulnerabilidade, ou ameaça, bem-sucedida (Stoneburner, Goguen, & Feringa, 2002).

A sétima atividade determina o risco. Esta atividade tem como objetivo avaliar o nível de risco para os diferentes sistemas. Segundo referem Stoneburner et al. (2002), pode ser revelada uma função através da determinação do risco para uma ameaça ou vulnerabilidade análoga. Essa função pode advir das seguintes probabilidades: probabilidade de uma fonte de ameaça tentar praticar uma determinada vulnerabilidade; da importância, ou extensão, do impacto deve com

[3] Capítulo 2.4 página 48.

sucesso uma ameaça-fonte exercer a vulnerabilidade e do ajuste dos controlos de segurança planeados para diminuir ou eliminar o risco. O risco pode ser medido através do desenvolvimento de uma escala de risco e uma matriz de risco-nível, tal como indica a Figura 19 sobre o sumário das categorias de impacto no negócio, (Stoneburner, Goguen, & Feringa, 2002).

Nível de Impacto	Definição
Nada ou Nenhum	Funções que podem ser interrompidas por tempos prolongados a custo muito reduzido ou quase nulo. Não existe nenhum impacto.
Pouco	Funções que podem ser interrompidas por tempos prolongados a custo reduzido, sendo que o impacto face à existência de uma falha de algum processo é muito pouco.
Medianamente ou Médio	Funções que podem realizar-se manualmente por um período prolongado com custo reduzido. Em caso de falha em algum processo o impacto é reduzido ou moderado para o próprio departamento ou para outro que dependa deste.
Bastante	Podem realizar-se manualmente durante um curto período de tempo. Em caso de falha existe um período em que o departamento ou outro que dependa deste, não conseguirá desenvolver o negócio.
Extremamente ou Extremo	Função que não pode ser substituída e têm uma tolerância muito baixa a interrupções. Resulta numa disrupção fatal que impede a atividade diária de toda a organização

Figura 19: Sumário das categorias de impacto e o seu nível de impacto

Fonte: (Adaptado de Ferrer)

Podemos classificar o impacto do negócio distinguindo quatro subcritérios, com classificações distintas na organização (Alves, 2009, p. 7):

- Imagem – classificação 4
- Financeiro – classificação 3
- Legislação – classificação 2
- Operacional – classificação 1

As classificações numéricas atribuídas a cada subcritério, foram as seguintes:

- Nada ou Nenhum – valor numérico 0,54 corresponde à classificação 1.

- Pouco - valor numérico 2,27 corresponde à classificação 2.
- Medianamente ou Médio - valor numérico 4,62 corresponde à classificação 3.
- Bastante - valor numérico 7,08 corresponde à classificação 4.
- Extremamente ou Extremo - valor numérico 9,25 corresponde à classificação 5.

Segundo referem Stoneburner et al. (2002), a oitava atividade indica os controlos que podem abrandar ou anular os riscos identificados, para uma redução do nível de risco aceitável.

Para finalizar, podemos indicar que Stoneburner et al. (2002), também recomendam, no final do processo de gestão de risco, a compilação da totalidade dos resultados, através de um relatório oficial com o objetivo de auxiliar os membros da administração e gestores a tomar uma resolução informada sobre os procedimentos orçamentais, políticos, processuais, operacionais e de gestão a decidir.

Além desta metodologia, podemos, ainda, referir a existência das seguintes normas para a gestão de risco:

- Norma ISO 31000 (Wikipedia, 2012), publicada em 13 de novembro de 2009:
  Define o conceito de risco como o "(…) efeito de incerteza sobre os objetivos (…)". Esta norma delineia o contexto interno e externo de uma dada organização e monitoriza, revê e comunica todas as atividades do processo de gestão de risco informando todos os proprietários de risco envolvidos na gestão de risco (Mrasmussen, 2009). Refere orientações genéricas para a conceção, implementação e manutenção de processos de gestão de riscos em toda a organização. Menciona a constatação de um padrão para a implementação de gestão de risco que pode ser aplicado a qualquer entidade (pública ou privada) e a qualquer atividade de negócio. Esta norma oferece a melhor estrutura prática e de orientação para qualquer operação de gestão de risco.

- Norma ISO 27005:2008 (Portal, 2008):
  Esta norma alcança a gestão de riscos de segurança de informação. Esta norma fornece orientações para a gestão de riscos de informações e é aplicável a todos os tipos de organização para suportar os requisitos dum sistema de gestão de segurança de informação definido pela ISO 27001.

2.2.4 **Análise de Risco**

Tal como referem Silva et al. (2010), a análise de risco é um processo que tem como objetivo gerar informação de modo sistemático para delimitar o grau de exposição da organização aos diferentes riscos aos quais está exposta permitindo ao Gestor de Topo sustentar uma tomada de decisão informada relativamente aos controlos de segurança a implementar. De modo a evitar investimento em segurança supérfluo, a análise de risco propõe-se a detetar os ativos da organização, assim como, as ameaças e as vulnerabilidades desses ativos e deste modo vão encontrando os pontos mais frágeis do SI. A análise de risco tem como objetivo principal fornecer dados que permitem à administração e liderança da organização uma visão clarificadora da sua atual situação para apoiar a tomada de decisões. Esta análise também permite identificar os eventos a ocorrer ou aqueles que podem vir a ocorrer e demarcar o seu impacto na organização. Uma análise de risco deve ser efetuada nas seguintes situações: quando a organização inicia um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou uma relação de parceria. Neste processo de análise de risco devem estar envolvidos especialistas em análise de risco e especialistas no negócio da organização. Devido à estrutura dinâmica que envolve a organização a análise de risco deve ser concretizada no menor espaço de tempo possível. O risco envolve os três seguintes elementos:

- Evento
- Probabilidade
- Impacto

Podemos dividir o risco em dois setores: o risco de negócio que está ligado a fatores externos à organização (aspetos económicos, legais, competitivos, entre outros) e o risco operacional que está ligado às operações internas na organização. O risco de negócio é um tipo de análise que suporta a tomada de decisões estratégicas da organização.

Podemos classificar o risco em cinco categorias, tal como indicamos na Figura 20 fontes caraterísticas do risco por categoria.

Categoria do risco	Fontes de risco
Técnica	Integração e interfaces Projeto de «*software*» Segurança Deteção de falhas Alterações no ambiente operacional Complexidade do sistema Recursos únicos e especiais
Programática	Disponibilidade de materiais e pessoas Qualidade técnica do pessoal Impacto ambiental Mudança de natureza politica Estabilidade das partes envolventes na mudança Mudanças de legislação Perfil de financiamento
Suporte	Segurança no sistema Suporte a recursos computacionais Dados e interoperabilidade Recursos humanos Equipamentos
Custo	Sensibilidade: ao risco técnico; ao risco de suporte; a riscos de cronograma; Margens Erro de estimativa
Cronograma	Sensibilidade: ao risco técnico; ao risco de suporte; a riscos de cronograma; Erro de estimativa Número de caminhos críticos

Figura 20: Fontes caraterísticas do risco por categoria

Fonte: (Adaptado de Nakashima & Carvalho, 2004)

2.2.5 **Metodologia - Análise de Risco**

Existem os seguintes modos de efetuar a análise de risco que podem ser integradas para aperfeiçoar os resultados, de modo independente:

- Análise de Processo38[4] – Referente à análise dos processos, abrange os controlos de gestão de riscos tendo como ponto de partida o "design", possibilitando alcançar conclusões sobre problemas constantes, ou habituais que se repetem ao longo do tempo;

- Análise Técnica39[5] – Atua sobre os ativos e as suas configurações, na tentativa de definir desvios dos padrões estabelecidos;

[4] Exemplo na Análise de Processo38 - o gestor de rede pode realizar alterações sem controlo associado.

[5] Exemplo na Análise Técnica39 - problemas de configuração de «firewall».

- Conjunto Análise40[6] – Posteriormente a uma revisão dos processos e respeitantes formas e mecanismos de controlos e a sua adequação é realizada uma revisão técnica para comprovar os resultados. A execução de uma Análise de Risco gera um documento, um relatório com indicações, que permite à organização controlar a sua estratégia e identificar os procedimentos a executar em curto, médio e/ou longo prazo. A Risk Management Standard, 2002 é uma Norma de Gestão de Risco que salienta a importância de apresentar os riscos de modo estruturado, para tal foi criada a Figura 21 com a Tabela 10 na qual são descritos os riscos com o objetivo de simplificar a descrição desses riscos e a sua avaliação.

Designação do risco	Descrição
Âmbito	Descrição qualitativa de acontecimentos, como dimensão, tipo, número e dependências
Natureza do risco	Estratégicos, financeiros, operacionais, de conhecimento ou conformidade
Intervenientes	Intervenientes e respetivas expetativas
Quantificação	Importância/relevância e probabilidade
Tolerância para o risco	Potencial de perda e impacto financeiro do risco
Tratamento e mecanismos de controlo	Principais meios através dos quais o risco é gerido
Possíveis ações de melhoria	Recomendações para redução do risco
Desenvolvimento de estratégias e políticas	Identificação da função responsável pelo desenvolvimento de estratégias e políticas

Figura 21: Tabela 10 Descrição dos Riscos

Fonte: (A Risk Management Standard, 2002, p. 7)

António Brasiliano (2009), indica que é na análise de risco que são estabelecidos os critérios importantes para dois princípios: o Impacto e a Probabilidade. A interseção destes dois princípios tem como resultado uma Matriz de Riscos, tal como se observa na Figura 22 e 23 com o exemplo Matriz Impacto e Magnitude na Análise de Riscos.

[6] Exemplo no Conjunto Análise40 - existem controlos de mudança na rede e na análise dos dispositivos é suficiente.

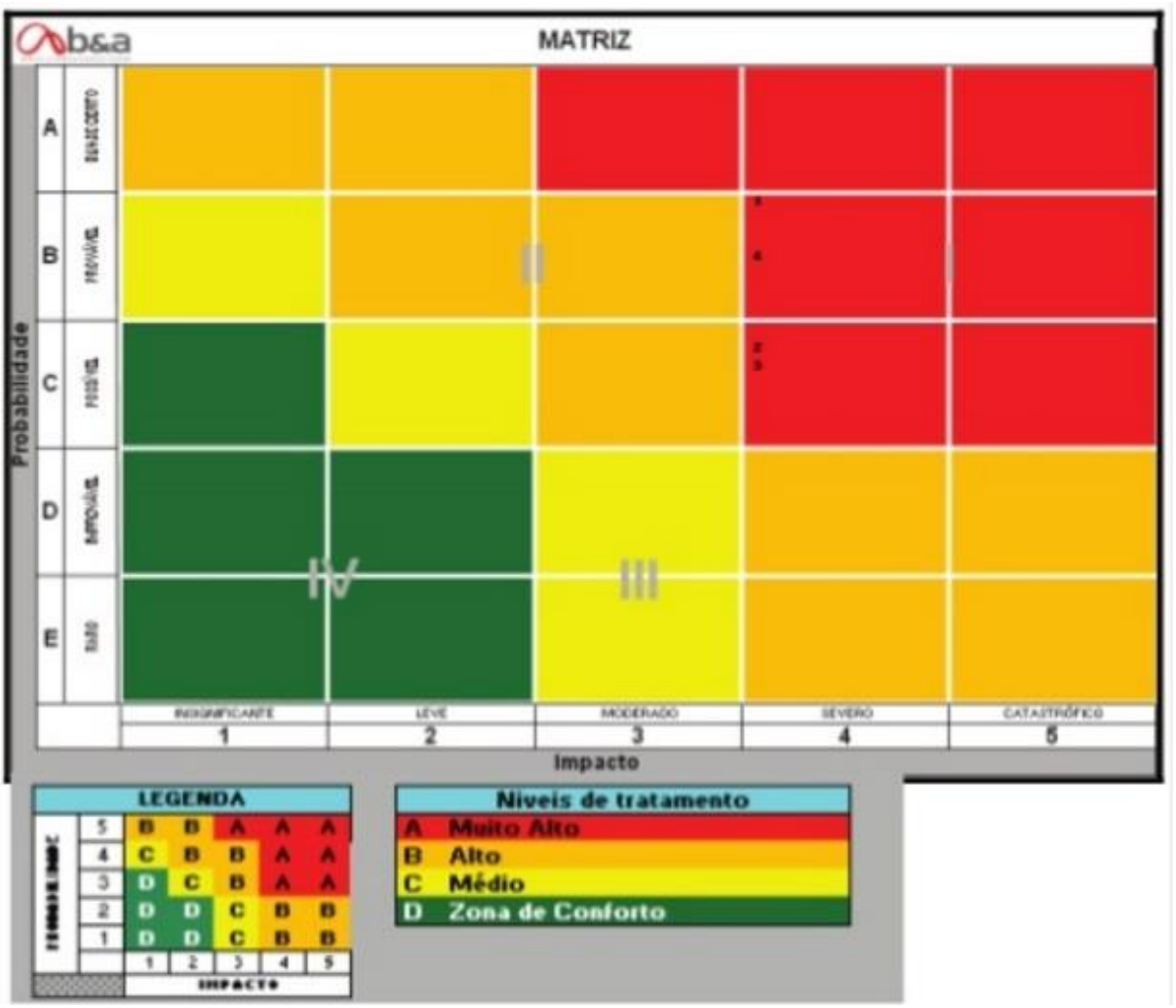


Figura 22: Exemplo Matriz Impacto x Magnitude - Análise de Riscos

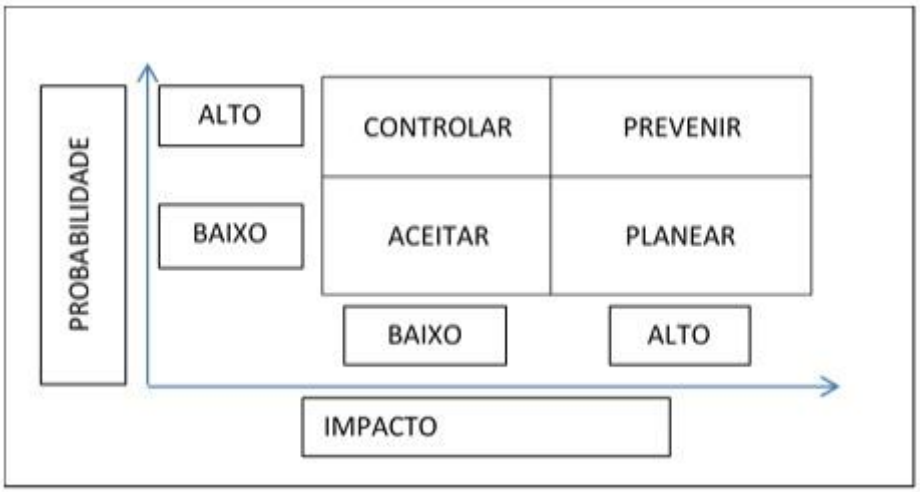


Figura 23: Matriz de Risco

Fonte: (Adaptado de Gallagher, 2003, p. 47)

De modo sucinto, pode-se compreender da Figura 22 e 23, (Matriz Impacto x Magnitude - Análise de Riscos e Matriz de Risco), que mediante a análise métrica Magnitude x Impacto o gestor irá posteriormente tomar decisões corretivas e consoante a análise métrica [(Magnitude x Impacto) x Probabilidade] irá tomar decisões preventivas.

O Project Management Body of Knowledge (PMBoK) (Project Management Institute, 2004) é um dos modelos de risco utilizados. O PMBoK, divulgado pelo Project Management Institute (PMI), trata de um conjunto de práticas, compiladas na forma do Guia PMBoK (Wikipédia 2012), de gestão de projetos e compõem a base do conhecimento na gestão de projetos do PMI.

2.2.6 **Normas Principais**

- BS ISO 31100 – Esta norma de gestão de riscos é um código de práticas e orientações para a aplicação da BS ISO 31000 no qual é descrito o processo de gestão de riscos. Este código pode ser interpretado e adaptado ao modo de trabalho de cada grupo de forma adequada para aumentar a consistência e a comunicação na organização (British Standards Institution, 2011);

- ISO 27005 – Designação da série "standard" principal 27000, cobre informação de gestão de riscos de segurança. Esta norma oferece orientações para a informação de gestão de riscos de segurança numa organização, apoia especificamente as formalidades de um sistema de gestão de informações de segurança definido pela ISO 27001;

- COBIT 5 – Esta norma é um "*framework*" de negócios para administração e gestão de TI. Esta versão incluí administração corporativa e técnicas de gestão. Para ajudar a aumentar a segurança e valor nos sistemas de informação esta norma fornece práticas globalmente aceites, ferramentas e modelos analíticos (Fagundes E. M., 1996-2012);

- ISO 27002 – Esta norma é a nova designação da norma ISO 17799. Trata-se de um código de práticas para a segurança da informação. Descreve centenas de controlos e mecanismos potenciais de controlo que podem ser executados, submetidos à orientação fornecida na ISO 27001, consoante a necessidade da organização. Esta norma também fornece um guia para o desenvolvimento de "(…) normas de segurança organizacional e práticas de gestão eficazes de

segurança e para ajudar a construir a confiança nas atividades entre organizações (…)" (ISO 27000 Directory, 2008);

• ITIL v.3 – Esta *framework* de melhores práticas sugere um sistema modular para completar a abordagem do processo e a abordagem técnica. Permite uma visão abrangente, completa e precisa, do estado da arte da segurança de TI;

• ISO/IEC 17799/2003 – Esta norma trata-se de um conjunto de orientações recomendadas para práticas na gestão de Segurança da Informação. Os objetivos da ISO/IEC-17799/2003 são os seguintes: integridade, disponibilidade das informações e confidencialidade, condições importantes para a segurança da informação. Além das caraterísticas já descritas, esta norma abrange também as seguintes caraterísticas: auditoria, não repúdio, autoridade, autenticidade, responsabilidade e legalidade.

2.4 **ANÁLISE/AVALIAÇÃO DE IMPACTO DE NEGÓCIO (BIA)**

A primeira fase de um plano BCP é a análise de impacto de negócio ou avaliação de impacto de negócio (análise BIA) e pode ser representado como um processo de negócio. A análise BIA consiste numa avaliação objetiva sobre o impacto financeiro da organização quando esta sofre uma falha da operação dos serviços de TI.

Segundo George Wrenn (2012), a análise BIA é um processo analítico cujo objetivo é apresentar negócios e impactos operacionais resultantes de qualquer número de ocorrências ou incidentes.

Sandra Alves cita, segundo António Celso Ribeiro Brasiliano[7], a análise BIA mantém uma visão estratégica contínua, priorizando os processos de negócio mais significativos da empresa ao nível do impacto no negócio e ao nível de tolerância, só após este processo inicia o planeamento dos procedimentos de contingência para obter uma definição mínima dos componentes a replicar ou reproduzir.

Deste modo, pode ser definida a análise BIA como um procedimento direto representado por técnicas e metodologias utilizadas para identificar, quantitativamente e qualitativamente o impacto dos seus efeitos de perda de uma paragem de negócios, não só relativamente ao número

[7] Diretor executivo da b&a, Brasiliano & Associados. Gestão de Riscos Corporativos.

de dias, mas também relativamente do ponto de vista financeiro, isto é, definir qual o tempo possível no qual a organização recupera de determinada quebra no negócio para voltar a praticar as suas operações dentro da normalidade (California Emergency Management Agency, 2011) (Pelant, 2005).

A TI e SI, no contexto atual deste estudo, a análise BIA determina, na organização, os sistemas e aplicativos críticos de tempo, as telecomunicações, os dados, o tempo de recuperação e os objetivos de ponto de recuperação. A análise BIA vai permitir, essencialmente, à organização medir os seus riscos contra os impactos, desse modo, essa informação determina onde e como a organização deve aplicar o seu orçamento disponível para a continuidade de negócio. É fundamental a organização possuir um conhecimento pormenorizado sobre todas as operações de negócio, isto é, para realizar a análise BIA é fundamental a compreensão dos processos de negócio e a influência que eles sofrem no contexto real pelos serviços de TI e SI.

Tal como podemos observar na Figura 24, tendo em conta o impacto no negócio e o tempo de tolerância o objetivo é organizar, ou mapear, a importância dos processos críticos e dar prioridade à sua restauração, ou recuperação (Alves, 2009).

BIA - BUSINESS IMPACT ANALYSIS
MÉTODO DE ANÁLISE DE IMPACTO NO NEGÓCIO

				Relevância do Impacto							Tolerância de Tempo	Status
				Imagem	Financeiro	Legislação	Operacional	NOTA	Média Ponderada Impacto	Nível de Impacto	Níveis de tolerância	Hot - Warm - Cold
	Área de Negócio	Processos	Processos de Interferência	4	3	2	2	11	-			
1	Auto Finance	Crédito Concessionárias	IT	4,0	5,0	3,0	5,0	47,0	4,27	SEVERO	6	HOT
2	Auto Finance	Rede Agência	**	3,0	3,0	3,0	3,0	33,0	3,00	MODERADO	5	WARM
3	Auto Finance	Digitação SP - RJ	**	2,0	2,0	1,0	2,0	20,0	1,82	LEVE	4	COLD

Figura 24: Exemplo de um ficheiro com análise BIA

Fonte: (Alves, 2009 p. 8)

A análise BIA tem especial interesse porque concede respostas às seguintes questões:

- Quais os riscos, no contexto real da organização, associados ao negócio?
- Esses riscos podem ser quantificados?
- Quais as providências que devem ser admitidas, em caso de desastre, para que o negócio continue funcional?

Quando é realizada uma análise BIA a organização deve ter em consideração a identificação das seguintes variantes:

a) Identificar as datas críticas e o impacto para o negócio numa linha temporal;
b) Identificar quanto tempo a organização iria demorar a sentir o efeito de uma paragem nessa situação;

Os níveis de tolerância ao tempo podem ser classificados de acordo com as Tabelas 2 e 3 seguintes:

Tabela 2: Modelo Genérico de Matriz de Exposição a riscos (probabilidade versus impacto)

Exposição			Impacto				
			0,54	2,27	4,62	7,08	9,25
			Nada (Insignificante)	Pouco (Reduzido)	Medianamente (Moderado)	Bastante (Elevado)	Extremamente (Catastrófico)
Escala	0,54	Nada	(BR)	(BR)	(RM)	(AR)	(AR)
	2,27	Pouco	(BR)	(BR)	(RM)	(AR)	(RE)
	4,62	Medianamente	(BR)	(RM)	(AR)	(RE)	(RE)
	7,08	Bastante	(RM)	(AR)	(AR)	(RE)	(RE)
	9,25	Extremamente	(RM)	(AR)	(RE)	(RE)	(RE)

Baixo Risco (BR) | Risco Médio (RM) | Alto Risco (AR) | Risco Elevado (RE)

Tabela 3: Relação do nível de tolerância e o tempo

Prioridade	RTO
Nada	Recuperação em 0 minutos – recuperação imediata
Pouca	Recuperação em 24 horas
Mediana	Recuperação em 48 horas
Bastante	Recuperação em 72 horas
Extremamente	Recuperação superior a 72 horas

O valor numérico da Prioridade utilizado na Tabela 3 (Relação do nível de tolerância e o tempo) é o utilizado na Tabela 2 (Modelo Genérico de Matriz de Exposição a riscos (probabilidade versus impacto).

a) Impactos financeiros e operacionais:
   Em caso de interrupção da atividade em determinado processo é fundamental descrever os impactos operacionais especificando a sua ligação com os custos financeiros associados.

b) Dependências:
   Listagem da totalidade dos componentes nos quais os processos assentam para serem garantidos sem interrupções. As dependências podem ser de origem interna ou externa.

c) Recuperação de tempo e objetivo[8]

d) Atuações alternativas:
   Para cada umas das atuações alternativas devem ser identificadas os dados seguintes:
   - Nome do procedimento;
   - Descrição;
   - Última data de teste ou de utilização;
   - "*Hardware*" indispensável;
   - Pessoal adicional necessário;
   - Tempo de utilização;
   - Tempo de implementação e o custo associado;

[8] RTO – Período de tempo a partir do qual a totalidade dos dados e serviços críticos devem estar operacionais. Descreve a quantidade de perda de dados medidos em tempo. O ponto no tempo no qual se deve recuperar os dados, tal como definido anteriormente pela organização, é o objetivo do ponto de recuperação. Normalmente é uma definição do que a organização estipula por "perda aceitável" numa situação de catástrofe ou desastre. Antes de um desastre, no qual podem existir perdas de dados, o RPO permite que a organização defina uma janela de tempo e o valor dos dados nessa janela de tempo que pode ser comparado com o custo da prevenção de desastres adicionais.

2.4.1 **Pontos-Chave da Análise Bia**

De modo resumido descreve-se cada um dos elementos tal como se observa na Figura 25 – Pontos-chave da análise BIA:

- Identificar a totalidade das instalações físicas da organização;
- Adquirir a lista de processos executados em cada uma das instalações e delimitar as que se relacionam, direta e indiretamente, com o serviço, ou seja, é necessário identificar os processos e as suas dependências;
- Descrever a importância de cada um dos processos através de uma análise de critérios sobre cada processo em cada instalação;
- Calcular através de inquéritos o RTO, POR e MTD para cada procedimento de instalação;
- Impor processos críticos a cada instalação, levando em consideração os níveis críticos de impactos para os negócios, RTO, RPO e MDT.

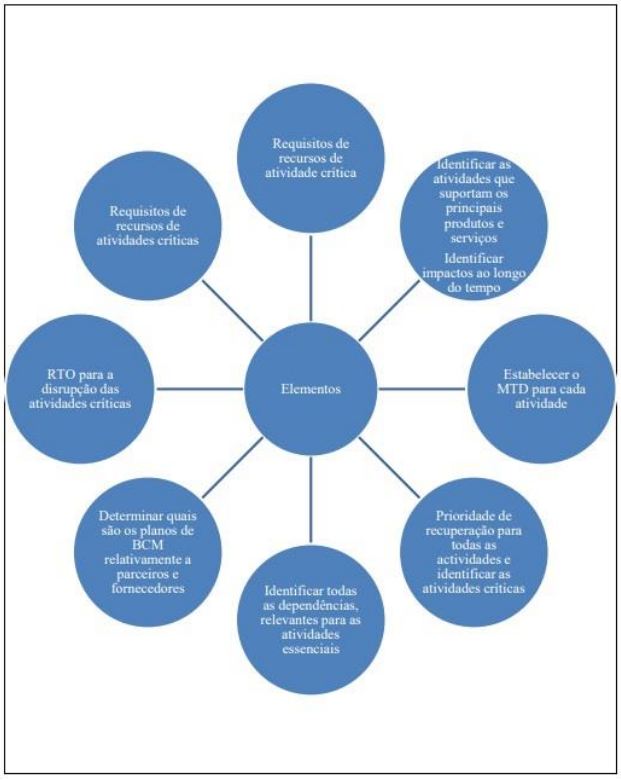


Figura 25: Pontos-chave da análise BIA

Fonte: (Adaptado de Estall, 2010)

2.4.2 **Metodologia**

O modelo apresentado na Tabela 4 assenta no processo de melhoria continua através de quatro atividades principais: planear, implementar, verificar e atuar.

Tabela 4: Atividades do modelo PDCA

Fonte: (ISO 22301, 2012)

Atividade	Descrição
Planear (*Establish (plan)*)	Estabelecer o plano de continuidade de negócio contendo as políticas, objetivos, objetos, controlos, processos e procedimentos relevantes de modo a atingir resultados alinhados com as políticas e objetivos da organização.
Implementar (*Implement and operate (do)*)	Implementar as politica, controlos, processos e procedimentos definidos na atividade anterior.
Verificar (*Monitor and review (Check)*)	Monitorizar e avaliar a performance face aos objetivos e politicas definidas e reportar os resultados para revisão da gestão que deverão determinar e autorizar as ações de melhoria.
Atuar (*Maintain and improve (Act)*)	Manter e melhorar o plano de continuidade da atividade através de ações corretivas baseadas na atividade de revisão, readaptando o plano, as politica e os objetivos.

Ou seja, tal como se pode observar na Tabela 5 a análise BIA deve ser considerada como um projeto de curta duração que abrange as fases seguintes: planear, recolher dados, análise dos dados, elaboração do relatório e aprovação da gestão de topo (Pelant, 2005).

Tabela 5: Metodologia de Análise BIA

Fonte: (Adaptado de Pelant, 2005)

Metodologia de análise BIA		
Fase	**Descrição**	
Planear	Objetivo	• Identificar a importância das funções de negócios • Identificar o impacto de interrupções ao longo do tempo • Identificar dependências críticas • Identificar recursos críticos
	Abordagem	• Recolha de dados • Análise de dados • Plano de projeto
	Recursos	• Patrocinador do projeto • Responsável do Projeto • Equipa de Projeto • Participantes do Projeto
	Compromisso da Gestão de Topo	• Aprovação • Envolvimento

Metodologia de análise BIA				
Fase	**Descrição**			
Dados	Preparar a estratégia de recolha de dados	Identificar os participantes	• Representantes de cada área funcional • Representante da Gestão de Topo	
		Determinar a abordagem	Entrevista	• Desenvolver guião de entrevista • Treinar entrevistadores • Validar guião
			Questionário	• Definir a estrutura do questionário • Desenvolver o processo de análise de dados • Desenvolver as instruções • Validar questionário
			Combinação dos dois métodos	
		Desenhar a infraestrutura	• Missão • Principais objetivos • Organização • Dependências • Impactos de interrupções ao longo do tempo • Potencial de mitigação de impacto	
	Realizar a recolha de dados	Preparar os participantes	• Emitir comunicado com objetivos • Apresentação Formal dos procedimentos • Distribuir as diretrizes da entrevista/agendamento de entrevistas ou distribuir o questionário • Indicar tempo de conclusão	
		Recolher dados	• Entrevista • Questionário	

Metodologia de análise BIA			
Fase	**Descrição**		
Dados (cont.)		Validar os resultados	• Abordagem da entrevista: o Organizar notas de entrevista o Identificar informações em falta o Preparar o resumo das notas o Confirmar os resultados por escrito • Abordagem de questionário: o Análise de consistência o Identificar informações em falta o Identificar "Bandeiras vermelhas"
	Análise de dados	Impactos de interrupções ao longo do tempo	• Quantitativo[41]: o Perda de receitas o Custo de sanções e multas • Qualitativa[42]: o Perda de satisfação do cliente o Perda de moral dos funcionários o Perda de controlo o Perda da segurança o Perda de imagem • Custo de relacionamentos
		Dependências críticas	• Dependências: o Internas o Externas • Interdependências
		Recursos críticos	• Pessoal • Informações • Processamento de informações • Comunicações • Equipamentos • Instalações • Fornecedores
	Organizar Informação	• Definir um sistema de níveis com base em resultados • Organizar as conclusões em camadas • Propor o plano de desenvolvimento estratégico para cada camada sobre as consequências de não fazer nada	

Metodologia de análise BIA		
Fase	**Descrição**	
Dados (cont.)	Elaborar relatório	• Fornecer informações oportunas de gestão para direcionar o desenvolvimento ou atualização de estratégias de recuperação, com base na lógica de negócio. • Listar os resultados da análise BIA • Identificar as recomendações de conclusões • Definir a próxima execução ou ações
Aceitação	Obter a aceitação da Gestão de topo	
Próximos passos	• Desenvolver uma estratégia de recuperação de negócios: o Âmbito o Abordagem o Recursos o Calendário	

2.4.3 **Objetivos**

De acordo com o *Business Continuity Institute* (Instituto de Continuidade de Negócios), Rodrigo Ferrer refere os quatro seguintes objetivos principais referentes à análise BIA para realização de uma análise de impacto:

- Compreender os processos críticos que suportam o serviço (a atividade da organização);
- Compreender a prioridade de cada um dos serviços e o tempo estimado de recuperação (RTO);
- Determinar o tempo de inatividade máximo tolerável (MTD)[9];
- Apoiar o processo para determinar as melhores e mais apropriadas estratégias de recuperação.

Para Doug Stoneman o melhor modo de colocar em prática a análise BIA é determinar os seguintes aspetos:

- Identificar os custos financeiros e os custos não financeiros;
- Estabelecer cada janela de tempo na qual a recuperação deve ocorrer;
- Identificar "*software*" e "*hardware*", dados e sistemas críticos;
- Produzir uma avaliação dos recursos necessários para a recuperação e continuação do negócio;
- Fornecer dados sobre os riscos do negócio (que podem não ter sido identificados anteriormente);

Segundo Doug Stoneman para atingir os objetivos acima descritos é necessário observar os processos críticos, realizar entrevistas ou questionários, rever e corrigir processos chave e fluxos de processo (Stoneman, 2003).

[9] MTD – Tempo máximo tolerável de inatividade (Maximum Tolerable Downtime). Indica o período máximo de tempo que um determinado processo empresarial pode estar inativo antes de colocar em risco a sobrevivência da organização.

2.4.4 **Benefícios**

Cleary (2005), destaca os seguintes benefícios da análise BIA:

- Estima os benefícios da aprendizagem, indicados em valores em euros;
- Permite a gestão de dados de modo a clarificar o âmbito de decisões;
- Fornece às equipas de formação orientações exatas sobre o campo de ação da formação;
- Trabalha em situações onde existem vários fatores de impacto;
- Suporta uma melhoria contínua que permite aos responsáveis pela formação ajustar de modo constante a formação.

2.4.5 Exemplo de Identificação de Recursos Críticos de TI

Swanson et al. (2002), identificam e referem, no suporte dos processos de negócio, os seguintes recursos como críticos:

- "Servidor de sistema operacional de autenticação / rede (necessário para que os usuários tenham acesso LAN);
- Servidor de base de dados (necessário para processar o sistema de Inventário);
- Servidor de e-mail e aplicativo;
- Cinco computadores desktop (para suportar cinco usuários do Inventário);
- Um hub (para suportar cinco usuários do Inventário);
- Cabeamento de rede;
- Energia elétrica;
- Aquecimento, ventilação e ar condicionado (HVAC);
- Segurança física;
- Facilidade."

3. METODOLOGIA DE INVESTIGAÇÃO

3.1 **ENQUADRAMENTO**

Sousa e Baptista (2011, p.53), destacam que se compreende por metodologia de investigação todo o processo de seleção da estratégia de investigação, com o qual se pretende atingir um ou mais fins. A seleção da metodologia depende do objetivo a atingir. Entre diversos tipos de metodologia destacam-se os seguintes:

- Métodos de investigação qualitativa;
- Métodos de investigação quantitativa;
- Métodos de investigação mistos.

Das já referidas metodologias, a investigação qualitativa abrange quatro categorias de tipos de estudo:

- Exploratórios;
- Explanatórios;
- Descritivos;
- Preditivos.

Sousa e Baptista (2011, p.58), destacam ainda que as abordagens qualitativas são adequadas a estudos de natureza exploratória, bem como o estudo de caso se enquadra nesses tipos de estudo. Desse modo, a metodologia adoptada para a realização da pesquisa foi estruturada na recolha de dados considerando a proposta de um estudo de caso com finalidade exploratória. Para atingir esse propósito foram observados alguns dados para a análise do impacto de negócio que destacam os problemas e as soluções para de recuperação de desastre.

3.2 **ESTRATÉGIA DE INVESTIGAÇÃO**

3.2.1 **Pesquisa Exploratória**

De acordo com António Carlos Gil (2008, p.26) a pesquisa tem um caráter pragmático e pode definir-se como um "(...) processo formal e sistemático de desenvolvimento do método científico. O objetivo fundamental da pesquisa é descobrir respostas para problemas mediante o emprego de procedimentos científicos".

A pesquisa exploratória é um procedimento metodológico caraterizado por uma abordagem qualitativa e contextual.

Segundo António Carlos Gil (2008, p.27), as "pesquisas exploratórias são desenvolvidas com o objetivo de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato."

Segundo Piovesan & Temporini (1995, p.321) a pesquisa exploratória é definida como um estudo inicial que se realiza com o objetivo de selecionar do melhor modo o instrumento de medida à realidade a estudar.

No entanto, a definição comum surge dos autores Theodorson & Theodorson (1970) que referem que a pesquisa exploratória é o estudo preliminar cujo objetivo base é familiarizar-se, ou contextualizar-se, com o fenómeno que está a investigar, para que o estudo possa ser preparado com melhor precisão e compreensão. O estudo exploratório permite ao investigador delimitar, com mais precisão, uma ou mais questões e formular uma ou mais hipóteses. Este estudo, também, permite escolher as técnicas adequadas às pesquisas e determinar as questões, conseguindo despertar o investigador para as potenciais dificuldades, apreciações e resistências[10].

Segundo Gil (2008, p.27) estes tipos de pesquisa adequam-se a situações nas quais não existe conhecimento da matéria em estudo "(...) apresentam menor rigidez no planeamento. Habitualmente envolvem levantamento bibliográfico e documental, entrevistas não padronizadas e estudos de caso. Procedimentos de amostragem e técnicas quantitativas de coleta de dados não são costumeiramente aplicados nestas pesquisas."

[10] Tradução realizada sobre a citação recolhida do artigo publicado por Piovesan & Temporini (Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública, 1995, p. 319).

Piovesan & Temporini (1995, p. 321) indicam que o propósito da pesquisa exploratória é "(...) conhecer a variável de estudo tal como se apresenta, seu significado e o contexto onde ela se insere."

No caso de pesquisas com o objetivo da realização de um trabalho académico, tanto os autores Linda Reis (2008) como António Carlos Gil (2008), referem como adequada a utilização da pesquisa exploratória por ponderarem que esta pesquisa possibilita ao investigador uma familiarização, ou contextualização, com a temática e o objeto de estudo, proporcionando maior facilidade na construção de questões pertinentes para o estudo.

3.1.2 **Estudo de Caso**

De acordo com Yin o estudo de caso é: "um dos empreendimentos mais desafiadores na pesquisa" (YIN, 2010, p. 23). Este método teve origem no campo da Medicina, e constitui hoje uma das principais modalidades de pesquisa qualitativa no campo das Ciências Humanas, Sociais e nas Tecnologias de Informação e teve os seus procedimentos estabelecidos de modo adequado a partir da obra do autor Robert Yin nos anos de 1990 do século XX.

Segundo Yin (2010, p. 39),

"(...) o estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente evidentes."

O método de estudo de caso conjetura o conhecimento do fenômeno a partir da exploração em profundidade de um único caso. Teve origem na pesquisa médica e psicológica, baseada na análise detalhada de um caso individual, com o objetivo de explicar a dinâmica e a patologia da doença investigada. Embora importado das Ciências Médicas, o estudo de caso tornou-se uma das principais modalidades de análise das Ciências Sociais (BECKER, 1999. p. 117), sendo também comum nas áreas de Assistência Social, Administração, Educação, Enfermagem, Planeamento Comunitário e Tecnologias da Informação (Yin, 2010, p. 24).

Em contexto de estudos referentes a organizações e as estratégias de gestão dos TI/SI é frequente a utilização do método de estudo de caso (Martins & Belfo, 2010). Segundo Martins & Belfo (2010) a utilização do estudo de caso na investigação em TI/SI decorre fundamentalmente por três motivos:

- A utilização do ambiente da organização para investigar;
- O entendimento sobre a natureza e complexidade dos processos em estudo;
- Um método apropriado numa área temática com poucos trabalhos conhecidos.

Segundo Sousa & Baptista (2011, p. 64), estudo de caso pode ser definido como a pesquisa de um tema único, num determinado tempo, contexto e atividade especifica sobre determinada Organização na qual o investigador recolhe informação pormenorizada, sendo deste modo um estudo único.

Segundo Linda Reis (2008) estudo de caso pode ser definido como "(...) uma técnica de pesquisa com base empírica (…) e consiste em selecionar um objeto de pesquisa, que pode ser um fato ou um fenómeno estudado nos seus vários aspetos (...)"

A Tabela 6 resume as principais caraterísticas sobre o método de estudo de caso. Esta tabela permite a obtenção de uma visão geral sobre os pontos positivos e negativos quando é utilizada esta metodologia.

Tabela 6: Principais Características sobre o Método Estudo de Caso

Fonte: (Martins & Belfo, 2010, p. 45).

Características principais do método estudo de caso
1. O fenómeno é examinado no seu ambiente natural.
2. Os dados são recolhidos através de diversos meios.
3. Uma ou poucas entidades são examinadas (pessoa, grupo ou organização).
4. A complexidade da unidade é estudada intensivamente.
5. Os estudos de caso são mais aconselhados para a exploração, a classificação e nos diversos passos de desenvolvimento de hipóteses associados ao processo de construção do conhecimento; o pesquisador deve ter uma atitude recetiva para a exploração.
6. Não há envolvimento de nenhum controle experimental ou manipulação.
7. O investigador poderá não especificar previamente o conjunto de variáveis independentes e dependentes.
8. Os resultados obtidos dependem muito do poder de integração do investigador.
9. Podem ocorrer mudanças na escolha do local e nos métodos de recolha de dados quando o investigador desenvolve novas hipóteses.
10. O estudo de caso é útil no estudo das questões "porquê" e "como" porque lidam com ligações operacionais para ser seguidas ao longo do tempo em vez de por frequência ou incidência.
11. O foco está nos acontecimentos atuais.

Tal como referido anteriormente, esta metodologia ajusta-se ao objetivo deste estudo visto ser fundamental identificar o impacto do contexto organizacional e do seu ambiente, recorrendo ao conhecimento dos conceitos sociais, ou para as pessoas. Para validar o resultado do estudo de caso é primordial assegurar a colaboração de toda a organização com o objetivo de conhecer melhor a mesma e de modo a contribuir para a formação de conhecimento dentro da mesma.

4. ESTUDO DE CASO

Este Capítulo tem como objetivo a definição da estrutura do desenho do Estudo de Caso e a justificação do motivo pelo qual foi escolhido como método de investigação. A recolha de dados foi realizada através da observação direta, no contexto da organização, através da análise da documentação técnica e dos procedimentos referentes à continuidade de negócio em vigor na mesma. Foram realizadas entrevistas de caráter informal, não estruturadas, cujo conteúdo não foi registado a pedido da organização por questões de confidencialidade. A pedido da organização será preservado o nome da organização, assim como todos os detalhes considerados de caráter confidencial pela organização.

4.1 CARACTERIZAÇÃO DA ORGANIZAÇÃO

Trata-se de uma sucursal portuguesa de uma empresa multinacional europeia da área financeira, especializada no crédito ao consumo realizado à distância. Esta organização fornece soluções de crédito clássico, *revolving*, consolidado e automóvel. A organização em questão opera através de canais à distância através da internet e telefone e não possui uma rede física de balcões. Atualmente a empresa tem cerca de 465 colaboradores que se dividem por sete direções na sua sede em Lisboa. Tem em carteira um número superior a 340 mil clientes com um volume de negócio aproximado aos 115.531.592€ e um importante papel na dinamização da economia e no emprego ao nível nacional. Sobretudo, neste modelo de negócio a componente de TI tem um papel fundamental devido aos contactos com os clientes serem realizados à distância, devido a esse fator qualquer *downtime* tem um impacto imediato neste modelo de negócio e na imagem que a organização transmite ao cliente. A organização opera em Portugal desde 1966 e no início da sua atividade não dispunha de equipamentos informáticos próprios, utilizava um sistema IBM AS400 que estava alojado numa empresa concorrente da área financeira, este processo de trabalho levantava questões relativas à confidencialidade, flexibilidade e concorrência. Para a gestão de topo desta organização, desde o início, era clara a necessidade de ser informaticamente independente para proteger os seus dados, sendo assim criado um departamento de informática com desenvolvimento de sistemas próprios, personalizados à medida, dentro da própria organização. Esta otimização permitiu à organização preencher as exigências e as aplicações de negócio que foram desenvolvidas

através da tecnologia *web base* que facilitou o acesso às aplicações apenas através de um *browser*. Simultaneamente ao desenvolvimento desse novo sistema foi utilizado o modelo ITIL que serviu de referência para os sistemas de gestão de TI para garantir a qualidade do serviço fornecido ao negócio.

4.2 **CARACTERIZAÇÃO DA INFRAESTRUTURA INICIAL**

Para alojar a infraestrutura utilizada pela organização foi criado um CPD instalado numa sala comum com as características seguintes:

- Paredes falsas em madeira;
- Chão falso, com duas unidades de A/C de insuflação de ar frio através do chão falso;
- Sistema de deteção e extinção de incêndios.

Porém, este sistema apresentava vários problemas devido ao CPD ser apenas uma adaptação numa sala comum e não uma construção de raiz com esse único propósito, entre os quais, destacam-se os seguintes:

- O material que constitui as paredes não é resistente ao fogo;
- O mau isolamento térmico;
- O chão falso é excessivamente baixo e impossibilita a correta circulação do ar frio, causando problemas de refrigeração.

O CPD alojava cerca de 38 servidores físicos que suportavam as aplicações de negócio e infraestrutura:

- *Cluster* SQL de dois nós com as bases de dados transacionais;
- IIS de suporte às aplicações de negócio;
- Um *domain controller*;
- Um *Mail server*;
- Um *Proxy server*;
- Um *Fax Server*;
- Um *Mail Relay*;

- Um *FTP Server*.

Composição do Equipamento de Suporte:

- Sistema de controlo de acessos.

Composição da Infraestrutura de Rede:

- Um *Core Switch*;
- Dois *Switchs* de apoio;
- Uma *Firewall*.

Composição da Rede Pisos:

- Um *Switch* em cada fração.

Composição do Sistema de armazenamento:

- Um SAN com duas controladoras;
- Dois *Switchs* de fibra;
- Um *Array* de discos.

Composição do Sistema de backup para tapes armazenadas no local e executado manualmente.

A Figura 26 representa o seguinte esquema implementado pela organização:

- Um *Switch* core ligado aos *Switchs* de piso, com uma *vlan* por piso;
- Duas DMZ para os serviços com comunicação para o exterior;
- Uma DMZ para a infraestrutura do *website* com ligação ao exterior dedicado por dois operadores diferentes através de BGP;
- Uma ligação ao sistema *lagacy;*
- Duas ligações dedicadas a *contact center* com serviços contratados;

- Ligações através de um link partilhado com o acesso à internet corporativo para os seguintes canais:
    - Gráfica responsável pelas comunicações físicas através de VPN;
    - Seguradora parceira através de VPN;
    - Serviço de informação de crédito utilizado no processo de análise por túnel SSH;
    - Serviço contabilístico remoto através de VPN o SMS-C das operadoras para envio de SMS;
- A totalidade dos canais de comunicação e energia utilizavam fisicamente o mesmo percurso de entrada no edifício.

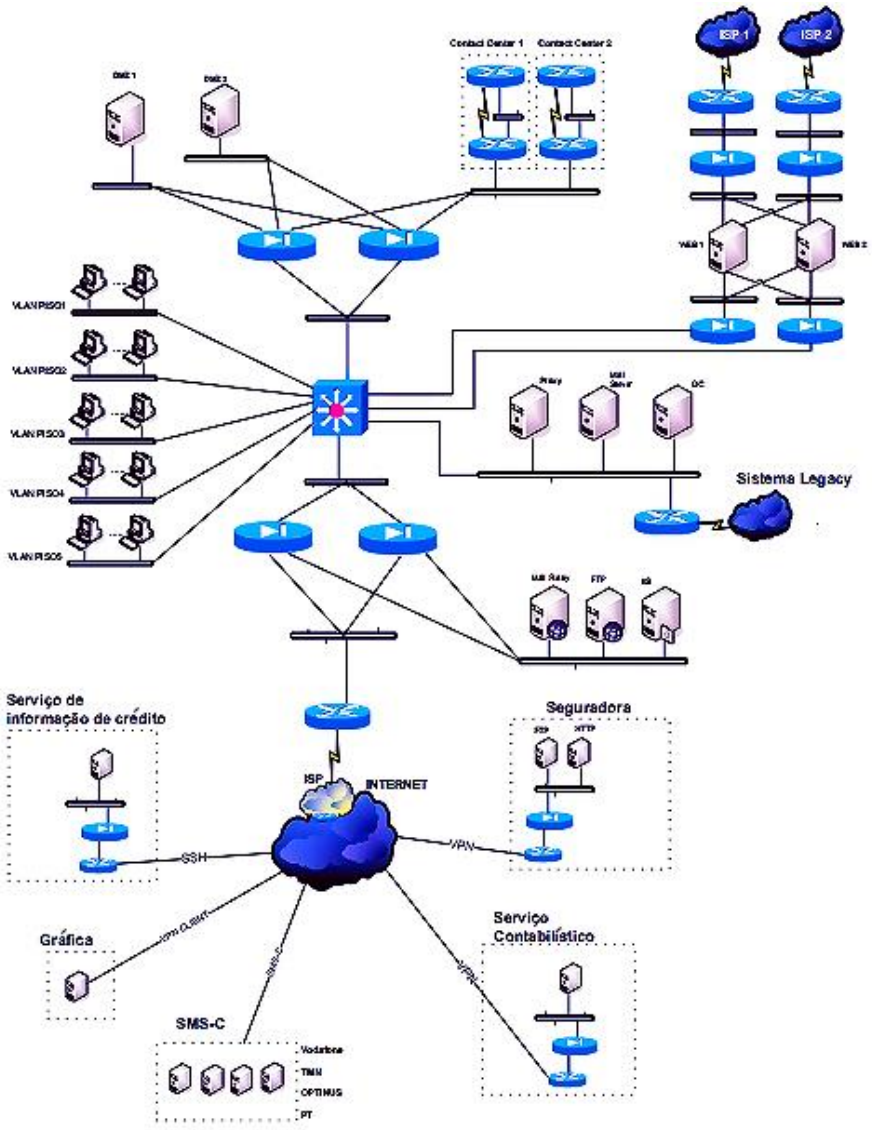


Figura 26: Representação Visual do Esquema da Rede da Organização

Composição da Infraestrutura de Voz:

- A gestão das chamadas era realizada internamente por uma central telefónica digital com elementos de *contact center*, ligada à rede pública através de primários de voz para chamadas para a rede fixa, e *comsat* para chamadas de rede móvel, tal como representa a Figura 27 seguinte.

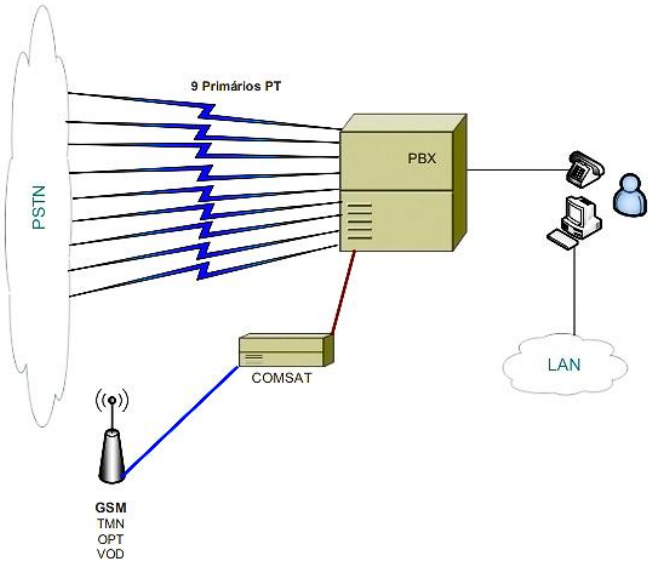


Figura 27: Representação Visual do Esquema da Infraestrutura de Voz da Organização

4.3. **PLANO DE CONTINUIDADE DA ATIVIDADE**

Sob o ponto de vista das TI e dos processos de negócio em caso de desastre foi realizado um estudo sobre o negócio e a sua infraestrutura através de uma recolha dos requisitos necessários para promover soluções que garantam a continuidade da atividade de modo a poder ser realizado o plano de continuidade da continuidade.

4.3.1 **Análise Inicial**

Neste estudo inicial, de modo a melhorar a perceção dos processos críticos para a organização, foram realizadas as funções descritas a seguir.

- Compreender as necessidades do negócio através da observação do próprio contexto de trabalho, nas diferentes direções da organização, para perceber os processos e a sua análise para a cadeia de valor do negócio. Para tal, foram esquematizadas as seguintes estruturas:

  - Responsabilidades principais;

  - Principais interdependências;

  - RTO, RPO, número mínimo de postos de trabalho correspondente a cada macroprocesso e o seu nível de criticidade;

  - Impactos de uma paragem, para as diferentes áreas da direção;

  - Circunstâncias críticas;

  - Sistemas de suporte com respetivo RTO e RPO e as suas aplicações;

  - Mínimos recursos.

- Esquema das aplicações com a infraestrutura que as suporta, assim como, respetivos RTO e POR (tendo em conta a análise do que foi referido e observado no contexto da organização).

- Apurado o resultado sobre a análise efetuada foi elaborado um BIA com a estrutura seguinte.

  - Breve contextualização sobre o enquadramento do negócio da organização, a sua missão, valores, estrutura orgânica, informação financeira e administração ou governação.

  - Registo de cada uma das seguintes direções:

    - Descrição sumária sobre a função da direção;
    - Os serviços da direção;
    - Interdependências principais;
    - Os impactos e os riscos causados por uma paragem;
    - Número de trabalhadores efetivos;
    - Os momentos críticos;

- Objetivos para a recuperação: recursos humanos, equipamento informático, linhas telefónicas, linhas de fax, fornecedores externos, processos manuais alternativos, registos críticos, tempos de recuperação e respetivas aplicações necessárias, atividades críticas posteriores ao desastre;
- RTO e RPO e respetivo resumo de todas as aplicações identificadas;
- Informação de todas as direções e respetivo resumo da informação.

- Análise de risco do centro de dados através do documento de análise dos riscos do CPD dentro do seguinte contexto:

  - Localização;
  - Espaço físico;
  - Segurança física;
  - Sistemas mecânicos;
  - Sistemas elétricos;
  - Sistemas de monotorização;
  - Sistemas de infraestruturas;
  - Sistemas de segurança e proteção contra incêndios.

4.3.2. **Análise de riscos físicos**

Na análise de riscos físicos consideraram-se três géneros de desastre, tal como se pode ver na Figura 28:

- Riscos Físicos:
  - O edifício da empresa localiza-se próximo ao aeroporto da portela e contíguo a edifícios habitacionais e de serviços cuja utilização é desconhecida por parte da empresa;
  - A Localização da empresa encontra-se em zona de risco sísmico;
  - Foram encontradas caixas de cartão no CPD e ausência de vídeo vigilância no acesso ao CPD;
  - O equipamento encontra-se espalhado pela sala e não está devidamente organizado;

- O edifício tem locais de fácil acesso para utilização, caso sejam necessários para finalidades de intrusão.

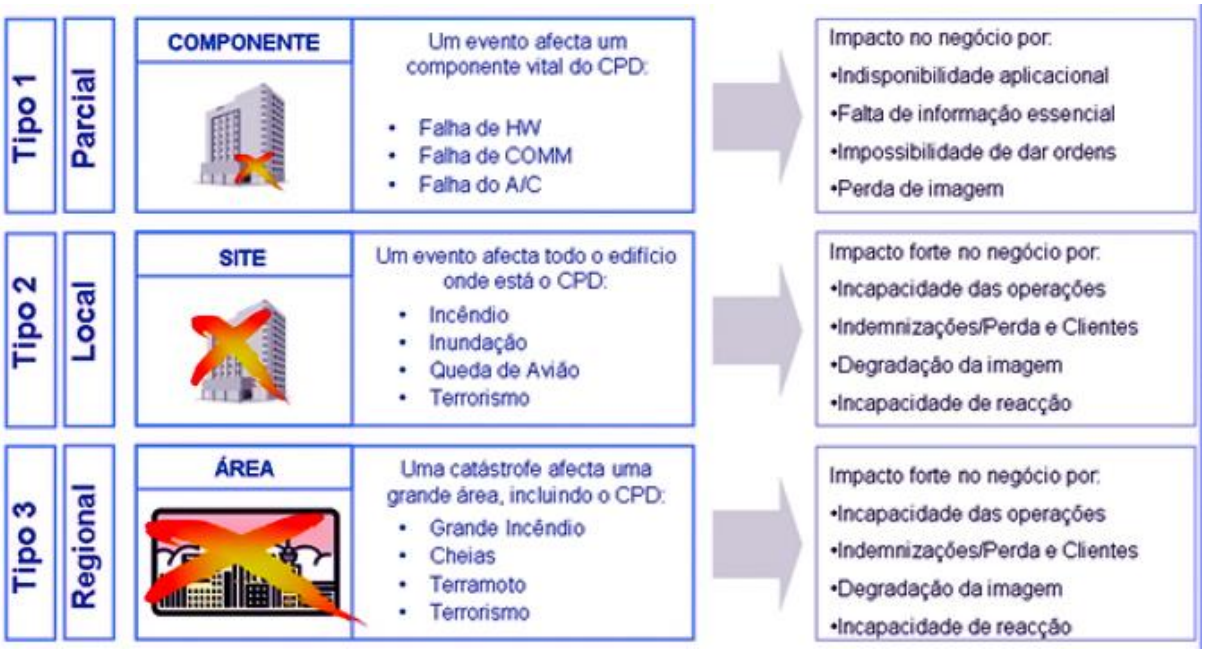


Figura 28: Três Géneros de Incidentes Interruptivos

- Sistemas Estruturais:
- Existe fragilidade e facilidade para forçar a abertura da porta de acesso ao CPD;
- Os cabos do CPD passam pelo teto com aberturas não seladas e não protegidas com material antifogo;
- O CPD está organizado em divisórias com vidro, sem resistência ao fogo, representando perigo de intrusão e risco em situações de incendio, ou em caso de ativação do sistema de extinção o vidro representa o perigo de partir e potenciar maior facilidade de propagação do incendio;
- A tubagem da sala de UPS tem a tubagem visível e apresenta risco de inundação;
- A sala é constituída por paredes finas, com pouca resistência ao fogo, com níveis de condensação da umidade elevados;
- A sala da UPS pode apresentar riscos em caso de inundação devido a não ter chão falso.
- O CPD tem um teto falso que se encontra solto em diferentes pontos constituindo risco de queda em pessoas ou equipamentos.

- Sistemas de Proteção de Incêndio:
  - Contrariamente à sala de CPD a sala de UPS não tem um sistema para deteção e extinção de incêndios.

- Sistemas Mecânicos:
  - Inexistência de sistema de renovação, ou circulação, de ar e extração de fumo;
  - O CPD e a sala da UPS, não têm um sistema de deteção de água por baixo do chão falso;
  - Não existem aberturas para o arrefecimento em todos os bastidores;

- Sistemas Elétricos:
  - Os quadros elétricos dentro do CPD apresentam risco de incendio e em caso de emergência são de acesso difícil;
  - A carga apresentada pela UPS é de 92% e a percentagem que deveria apresentar no máximo seria entre 75% a 80%;
  - Inexistência de gerador a diesel;
  - A UPS alimenta a totalidade do edifício, inclusive o CPD, existindo risco de ligação de um equipamento que cause interferência na rede elétrica numa tomada de socorro.

- Monitorização:
  - Inexistência de um sistema centralizado para agrupar alarmes dos detetores de incendio e águas;
  - Inexistência de um sistema de alarme na UPS que pode provocar a falta de aviso.

- Segurança Física:
  - O CPD não tem sistema de vídeo vigilância.

4.3.3 **Análise de Impacto no Negócio**

Por motivos de confidencialidade, da empresa em questão, os pormenores da análise de impacto de negócio não serão mencionados.

Tal como se pode observar na Tabela 7, ao longo desta fase identificaram-se os seguintes aspetos:

- Macroprocessos críticos para o negócio das respetivas áreas de negócio;
- Macroprocessos de negócio críticos ou o impacto de falhas nas áreas;
- RTO - Tempo máximo de paragem tolerável;
- RPO - Tempo máximo de perda de dados tolerável;
- Quatro níveis de criticidade.

Tabela 7: Níveis de Criticidade da Organização

Nível de Criticidade	Critério de seleção dos Processos por Criticidade	Requisitos de Recuperação dos Processos no Plano de Continuidade
NIVEL 1 **(Funções críticas)**	Tempo máximo de indisponibilidade, menor ou igual que 1 Dia. Dimensão do Impacto da Contingência: ALTO Impacto de uma perda de dados ALTO e nível de atualização indeterminado.	**Recuperação da função operacional até 1 Dia.** **Perda de dados aceitável: último *Backup* guardado fora do *site*. (dia anterior)** **Integridade dos dados garantida**
NIVEL 2	Tempo máximo de indisponibilidade, de 1 dia a 3 Dias. Dimensão do Impacto da Contingência: ALTO-MÉDIO Impacto de uma perda de dados ALTO e nível de atualização indeterminado.	**Recuperação da função operacional entre 2 a 3 Dias.** **Perda de dados aceitável: último *Backup* guardado fora do *site*. (dia anterior)** **Integridade dos dados garantida.**
NIVEL 3	Tempo máximo de indisponibilidade, 3 A 7 Dias. Dimensão do Impacto da Contingência: MÉDIO-BAIXO	**Recuperação da função operacional entre 4 a 7 Dias.** **Perda de dados aceitável: último *Backup* guardado fora do *site*. (dia anterior)**
NIVEL 4 **(Restantes Funções e Processos)**	**Tempo máximo de indisponibilidade > 7 Dias.** **Dimensão do Impacto da Contingência: BAIXO**	**A recuperação poderia ser feita em mais de 7 dias poderia não ser recuperado em situação de contingência**

Em suma, sobre os níveis de criticidade da organização, foram apurados os seguintes resultados:

- Três serviços com nível de criticidade 1;
- Quatro serviços com nível de criticidade 2;
- Um serviço com nível de criticidade 3;
- Oito serviços com um nível de criticidade 4.
-

Foram registados, também, como necessidade de negócio os seguintes resultados:

- Um RTO mínimo de um dia e máximo de 30 dias;
- Um RPO mínimo de 0 dias e máximo de 8 dias.

4.3.4. **Estratégias de Recuperação**

Com base no que foi apurado nos pontos anteriores foram avaliados diversos cenários de recuperação com suporte em cenários conceptuais, tal como se pode observar na Figura 29 considerando os *tiers* de recuperação definidos pelo grupo SHARE em 1992 (SHARE Inc., 2007).

Concluiu-se a existência das seguintes aplicações, após a divisão das aplicações/serviços pelos diversos *tiers:*

- 28 aplicações *tier* 2-3
- 2 aplicações *tier* 1

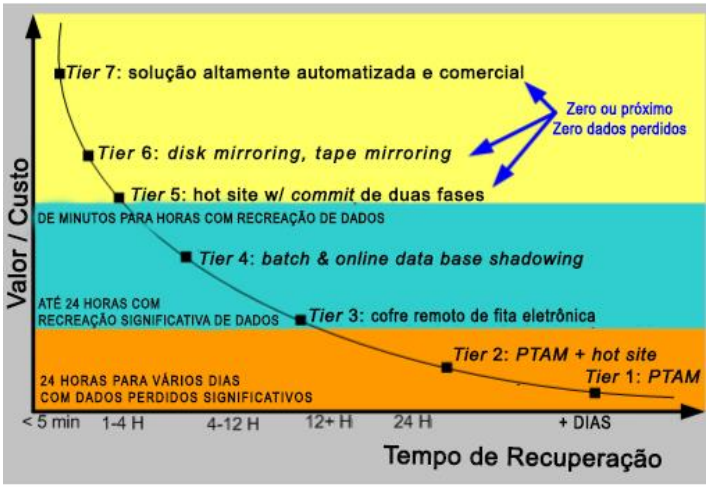


Figura 29: *Tiers* de recuperação

Fonte: (Adaptado de SHARE Inc, 2007)

4.3.5. **Identificação de Cenários**

Face à análise efetuada e referida anteriormente e aos requisitos de negócio foram ponderados três cenários viáveis para garantir a continuidade de negócio em caso de desastre. Para a ponderação desses cenários foram identificados os recursos críticos de servidores para recuperação do ambiente de produção da organização, nomeadamente: *SAN*, *LAN e WAN*.

4.3.5.1. **Estratégias para a Recuperação**

1º Cenário *Cold Site*:

Cold Site - Cenário sustentado na transferência de *tapes* para um *site* secundário sem infraestrutura instalada.

Recursos Essenciais

- Seleção de local alternativo para armazenar a recuperação de todas as cópias de dados críticos.
- O equipamento crítico e as linhas de comunicação podem não estar disponíveis no local alternativo que foi selecionado para armazenar a recuperação de cópias de dados críticos.

Processo de *Backup*

- *Backup* de todos os dados críticos efetuado em duplicado.
- O primeiro duplicado é mantido uma cópia no CPD para a recuperação local.
- O segundo duplicado é enviado para o centro de recuperação.

Processo de Recuperação

- O processo de recuperação e de gestão pode ser complicado.
- Para determinar os procedimentos de recuperação das aplicações é necessário o envolvimento da equipa aplicacional.
- O tempo de recuperação pode ser alto e de difícil previsão.
- Este cenário satisfaz os requisitos de aplicações *tier* 1.

2º Cenário *Warm Site*:

Warm Site – Cenário sustentado na transferência de *tapes* para um *site* remoto com infraestrutura e com possibilidade de iniciar através de um pedido.

Recursos Essenciais

- Seleção de local alternativo para armazenar a recuperação de todas as cópias de dados críticos.
- O equipamento crítico para recuperação do sistema de informação é partilhado e facultado após o desastre.
- Linhas de comunicação.

Processo de *Backup*

- *Backup* de todos os dados críticos efetuado em duplicado.
- O primeiro duplicado é mantido uma cópia no CPD para a recuperação local.

- O segundo duplicado é enviado para o centro de recuperação.

Processo de Recuperação

- Em situação de ocorrência de desastre todos os recursos críticos são facultados de imediato.
- Processo de recuperação de dados é similar ao realizado localmente, numa operação normal das equipas de suporte.
- O processo de recuperação e de gestão pode ser complicado.
- Para determinar os procedimentos de recuperação das aplicações é necessário o envolvimento da equipa aplicacional.
- O facto dos equipamentos ficarem disponíveis permite reduzir substancialmente o tempo de recuperação.

3º Cenário *Hot Site*:

Hot Site - Cenário sustentado pelos *backups* transferidos, ou executados em tempo real, para um site remoto com toda a infraestrutura operacional.

Recursos Essenciais

- Seleção de local alternativo para armazenar a recuperação de todas as cópias de dados críticos, identificado como o centro de recuperação em situação de desastre.
- O equipamento crítico para recuperação do sistema de informação é dedicado e deve estar preparado para entrar em atividade.
- Linhas de comunicação para transferência de dados entre os dois centros para a continuidade de negócio.
- *Tape drives* e *cartridges* suplementares, dependendo do caso.

Processo de *Backup*

- Disponíveis várias tecnologias de *backup*.
- Quando são utilizados processos como *Disk Copy*, Alta Disponibilidade, entre outros, pode ser realizado o *backup* da informação que existe no Centro de Recuperação, deste modo pode ser evitada a realização de *backups* duplicados, tanto no Centro de Produção, como também, no referente transporte.

Processo de Recuperação

- Em situação de ocorrência de desastre todos os recursos críticos devem ser disponibilizados para utilização.

- O processo de recuperação está dependente do cenário utilizado.
- No caso de *Disk Copy* os sistemas são iniciados tal como no Centro de Produção em caso de falha de eletricidade (tendo que recuperar apenas os dados em falta).
- No caso de *mirroring* o tratamento é idêntico com o benefício de não existir necessidade de recuperar dados.
- Nos casos de alta disponibilidade é possível, de modo quase automático, ter os sistemas em atividade.

4.3.5.2 **Documentação do Plano Continuidade do negócio**

Após a análise inicial foram criados e preservados atualizados os seguintes documentos de suporte à continuidade de negócio:

- Modelo de Gestão – Descreve os procedimentos sobre o método de gestão dos documentos que integram o plano de continuidade do negócio.
- Plano de Recuperação de Negócio – Descreve pormenorizadamente os procedimentos a realizar, pelas equipas de recuperação e respetivos *managers*, para a gestão de crise com o objetivo de reativar de modo célere a atividade de negócio.
- Plano de recuperação dos Sistemas de Informação – Descreve pormenorizadamente os procedimentos a realizar, pelas equipas técnicas, para recuperar os sistemas *core*.
- Plano de Testes – Descreve os testes a efetuar com o objetivo de avaliar a eficiência dos planos de recuperação e identificar possíveis erros que devem ser detetados e corrigidos.
- BIA (Business Impact Analysis) – Documento que descreve, com informação pormenorizada, os impactos e necessidades de recuperação para cada área e processo critico de negócio.

Os já referidos documentos são verificados anualmente, ou sempre que necessário, e atualizados pela empresa.

Foi criada uma comissão de crise responsável pela apreciação, análise, aprovação e formalização dos respetivos planos individuais para as diferentes áreas da empresa que acompanha e garante a continuidade da atividade. A comissão de crise incluí a totalidade da direção da organização e é responsável pela continuidade do negócio.

4.4. **PRIMEIRA FASE - IMPLEMENTAÇÃO**

Perante os cenários de recuperação, nomeados anteriormente, os gestores da organização avançaram para a implementação da solução *hot site* e foi fabricado de raiz um novo CPD situado no edifício próximo ao do CPD que existia anteriormente. O novo CPD tem as seguintes caraterísticas:

- Norma EN60529 - Segurança e proteção contra jato de água IP X6;
- Norma EN1363 - Segurança e proteção contra incendio até 1090cº, F90;
- DIN 18095 - Segurança e proteção contra gases inflamáveis corrosivos;
- Norma EN60529 - Segurança e proteção contra poeira IP5X;
- Norma EN 1627/1630 - Segurança e proteção contra intrusão classe 3;
- Segurança e proteção contra colisão de 200kg de uma altura de 1.5 m após tempo de inflamabilidade de 30 minutos;
- Segurança e proteção contra entrada e saída de radiações de alta frequência comprovada pela universidade politécnica de Aachen, Alemanha.

Com o novo CPD as informações passaram a entrar por dois pontos diferenciados do edifício, com percursos distintos dentro da rede do operador e com uma nova instalação de um novo ponto de entrada de energia oriundo de um ramal distinto do fornecedor. Deste modo as ligações externas permanecem repetidas, tendo cada um dos CPDs pontos de comunicação com o exterior distintos.

Foi adicionada ao CPD novo uma nova UPS com capacidade para 1.5h/autonomia. Foi realizado um upgrade às baterias da UPS para proporcionar o aumento da sua autonomia para 4h. A totalidade dos equipamentos instalados possuem fontes de alimentação redundantes, sendo que cada uma das fontes está ligada a uma UPS que garante a redundância energética de alimentação.

Para garantir a alta disponibilidade de servidores foi admitida a virtualização, com a abordagem de servidores físicos passou a uma abordagem de servidores virtuais distribuídos por dois chassis alojados em cada um dos CPD, que devido à tecnologia Vmotion correm em qualquer *host* sem qualquer quebra de serviço. No entanto, a infraestrutura da totalidade dos servidores

virtuais foi calculada para ter capacidade de correr num único chassi. Nos servidores das bases de dados, que ficaram fora da virtualização, foram criados três clusters SQL com dois nós que permitem a redundância.

Foram instaladas duas SAN com baias de discos para suportar os dados apoiados por dois *switchs* de fibra que foram repartidos pelos dois CPDs para garantir, em caso de falha das SANs principais, a disponibilidade dos dados. Foram montadas duas SANs no antigo CPD e configuradas em *mirror* nas SANs principais, foi necessária a reconfiguração das áreas de acesso aos dados, caso exista indisponibilidade das SANs principais para permitir o acesso aos mesmos.

Tal como podemos observar na Figura 30 foi instalado um *switch* core no novo CPD para garantir a redundância de rede, ligado através de fibra ao *switch* core do antigo CPD. Foram configurados, nos *switchs* de piso, *trunks* em fibra para cada um dos *switchs* core com *spanning tree* ativo.

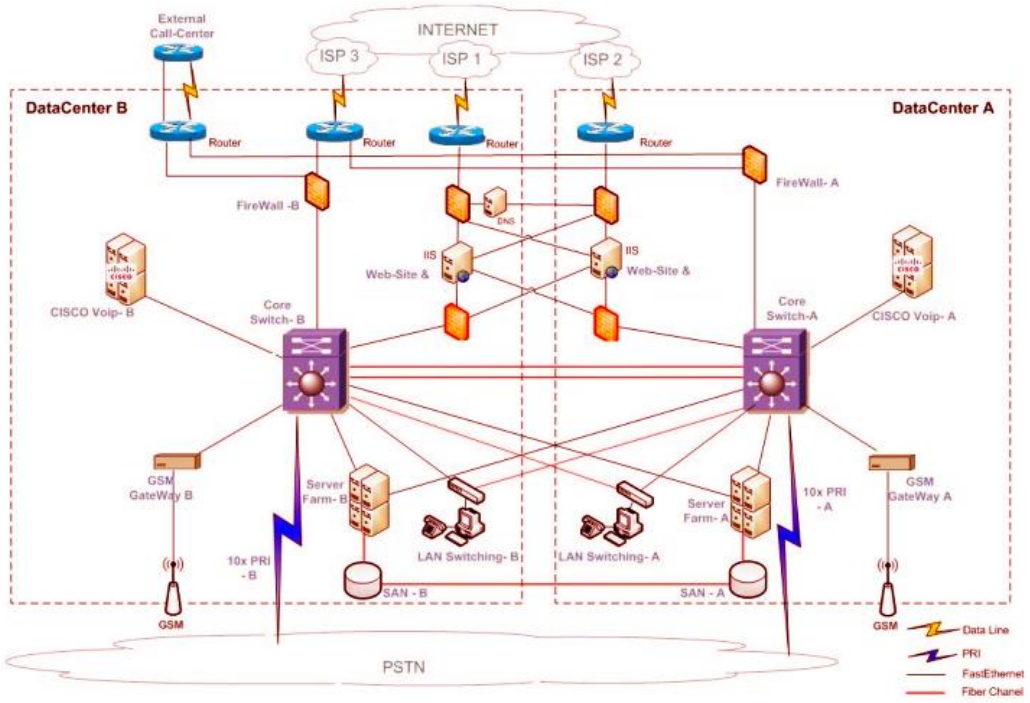


Figura 30: Esquema Lógico da Rede Primeira Fase de Implementação

Foi renovada a infraestrutura de voz para um sistema de VoIP com componentes redundantes e instalados dois conjuntos primários para assegurar as comunicações de voz com a rede fixa, assim como, dois comsat divididos pelos dois CPDs que garantem as comunicações com a rede móvel.

Pode ser observada na Figura 31 a estrutura de voz dividida pelos dois CPDs:

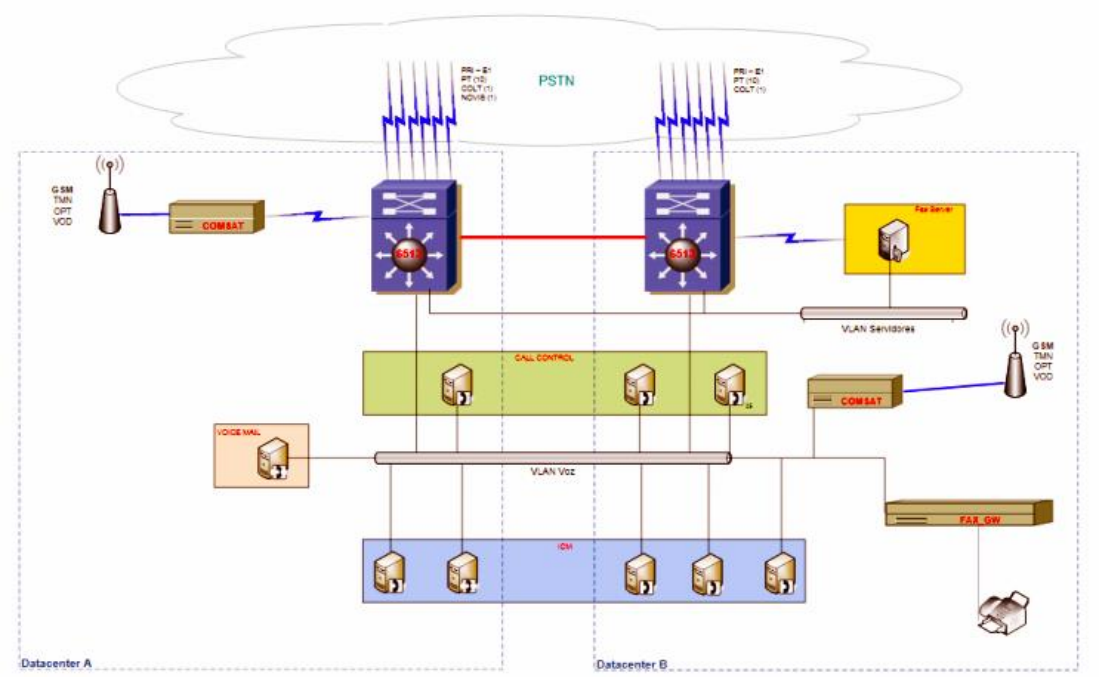


Figura 31: Esquema da Rede Voz na Primeira Fase de Implementação

Em caso de desastre ou acidente de exclusão, para garantir a disponibilidade da informação foi instalado um *robot de backups* com duas *pools de tapes*, uma foi instalada no *robot* e a outra externa corresponde à cópia da primeira *pool*. No caso de indisponibilidade do site principal foi contratado um serviço de *tape vaulting* no qual a segunda pool é enviada semanalmente para um cofre a 300 km de distância.

4.5. **Segunda fase - Implementação**

A solução implementada não garante uma proteção contra desastres de nível 3, apesar de ser de alta disponibilidade, deste modo, a solução passou pela criação de um espaço na área de Oeiras com 120 postos de trabalho e um novo CPD para alojar a infraestrutura redundante que

estava no antigo CPD, que passou a ser considerado como uma sala técnica. Nesta segunda fase de implementação foram realizadas algumas alterações na infraestrutura.

4.5.1. **CPD redundante**

O novo CPD foi construído com as particularidades seguintes, para proteção contra desastres do tipo 3:

- Norma EN60529 – Segurança e proteção contra jato de água IP X6;
- Norma EN1363 – Segurança e proteção contra incendio até 1090cº, F90;
- Norma EN60529 – Segurança e proteção contra poeira IP5X;
- Norma EN 1627/1630 - Segurança e proteção contra intrusão classe 3;
- Segurança e proteção contra gases inflamáveis corrosivos DIN 18095;
- Segurança e proteção contra entrada e saída de radiações de alta frequência comprovada pela universidade politécnica de Aachen, Alemanha.
- Segurança e proteção contrachoque de 200kg de uma altura de 1.5 m apos tempo de inflamabilidade de 30 min.

O novo CPD tem instalado um sistema de sensores de fumo e temperatura que permite detetar e extinguir incendio, colocados ao nível do teto e por baixo do chão falso, também tem uma nova UPS e baterias com duas horas de capacidade. O antigo CPD passou para a sala técnica com um s*witch* core para redundância e *switch* de distribuição de rede para o piso.

4.5.2. **Infraestrutura de Rede**

Com a topologia de rede, que passou a utilizar a tecnologia VSS para garantir os chassis do site principal e *portchannels* para interligar os equipamentos de rede, foi possível aumentar os níveis de estabilidade de redundância e diminuir a dependência de STP.

Infraestrutura de rede do site principal

Core Switch

- Passaram a ser utilizados dois módulos de supervisão em cada switch core;
- Os *switchs core*, do site principal, são agregados em VSS para garantir a performance e redundância.

Switch de Acesso

- Passaram a ser utilizados *portchannels* com um membro em cada chassis, para tirar benefício da tecnologia VSS e aumentar a largura de banda de 1 Gbps para 2 Gbps, deste modo ficaram menos dependentes da componente de STP.

Infraestrutura de rede do site secundário

Core Switch

- Dois módulos de supervisão para um core *switch*.

Switch Acesso

- Tal como no site principal utilizam-se *portchannel* para a ligação ao *switch* core.

Os dois sites são ligados em *portchannel* alcançando assim redundância e uma largura de banda superior que pode chegar a 20Gbps (com os dois *links*), e estabilidade superior devido a não utilização de STP.

Alterações à Configuração Global

Layer 2

• Tecnologia VTPv3, para permitir a propagação de vlans no *extended-range* e propagação da configuração 802.1s.

- Os dois cores estão em modo server;
- A totalidade dos equipamentos estão em modo cliente.

• A tecnologia STP 802.1s foi aplicada para resolver o problema de instâncias de STP, progredindo, deste modo, para a versão atualizada da tecnologia.

- A *root bridge* das instâncias de 802.1s tem como sequência, primário *core site* principal e secundário *site* secundário.

Layer 3

• O uso de HSRP v2, no qual, o primário é o *site* primário e secundário o *site* secundário.

Firewall

- Para manter a redundância foram instaladas, nos dois *sites*, firewall que funcionam em modo ativo/standby e utilizam instâncias virtuais.

4.5.3. **Infraestrutura de Servidores**

Foram obtidos, para a estrutura de servidores, três novos chassis (dois *fabric-interconnect* e dois MDS para cada CPD). O recurso foi dividido em dois *fabrics* por cada site, os *fabric-interconnect* permanecem configurados em modo *end-host* não participam na preferência da *root bridge* do domínio de STP. O mecanismo de *mac-learning* permanece desativado e é escolhido um *uplink* para processar todo o tráfego de *multicast* e *broadcast*.

Cada um dos *fabric-interconnect* possuem um *uplink* para cada nó do sistema VSS e estão agregados num *portchannel*.

Topologicamente cada um dos *fabric-interconnect* tem um *port-channel* para o *Core* controlando os mecanismos de redundância necessários. A conectividade com cada um dos *chassis* é realizada pela via de quatro canais de 10Gbps por IOM, complementarmente esses

quatro canais encontram-se associados por via do protocolo LACP. Na prática a conectividade entre o *chassis* e os *fabric-interconnect* é efetuada via FCoE.

4.5.4. **Infraestrutura SAN**

A infraestrutura SAN foi modernizada e passou a utilizar duas SANs e dois tipos de *storage* com tecnologias diferenciadas.

Duas *storage*, uma para cada *site* com as seguintes funções:

- Tendo em conta a performance e histórico de acesso aos dados foi realizada a disposição dos dados por camadas, nomeadamente três camadas com performances distintas nas quais:

  - Fast cache de 400Gb em SSD;
  - Tier 1 - SSD serve 2 % dos dados;
  - Tier 2 – SAS serve 32 % dos dados;
  - Tier 3 - NL SAS serve 66% dos dados.

- Recovery Point – Sistema de recuperação dos dados que possibilita a recuperação remota ou local realizada através da replicação de dados enviada para o site secundário.

Para além das funcionalidades já referidas, a segunda SAN usa um sistema em cluster para garantir a escrita nos dois sites ao mesmo tempo mediante volumes distribuídos e com uma replicação de dados quase em tempo real garantindo um RPO de minutos.

4.5.5. **Infraestrutura de *Backup***

Foi instalada uma tecnologia, com uma solução de backup para disco, que permite reduzir exponencialmente os tempos de backup diários. A infraestrutura de backups encontra-se dividida pelo site sede e o de recuperação (site sede primário, site de recuperação secundário que pode assumir o papel de primário caso seja necessário). São realizados backups diários sobre a totalidade da infraestrutura, inclusive das máquinas virtuais, e armazenados no sistema

de backup do site principal, também replicados para o sistema de backup do site secundário, nomeadamente com os seguintes tempos de retenção:

- Réplica backup diário – retenção 1 mês;
- Réplica backup semanal – retenção 1 mês;
- Réplica backup mensal – retenção 1 ano;
- Réplica backup anual – retenção 1 ano.

4.6. **TESTES**

Para confirmar a eficiência do plano de continuidade de negócio foi formulado e aprovado pela comissão de crise um plano de testes e um plano de execução desses testes com os respetivos registos e resultados.

4.6.1. **Plano de Teste**

O plano de teste deve assegurar os seguintes pontos:

- Simulação de uma situação de desastre real;
- Verificação da adequação dos dados e documentos para a recuperação guardados off-site;
- Capacidade das equipas de recuperação de realizarem as respetivas atividades e responsabilidades nos testes;
- Capacidade de recuperar as funcionalidades pretendidas;
- Determinação de condições válidas para a Recuperação em caso de desastre.

O documento sobre o Plano de Teste incluí três tipos de teste, nomeadamente:

- Caminho estruturado em papel - Simulação realizada em papel de uma situação interruptiva;
- Teste anunciado – Agendado para a recuperação da produção no CPD de recuperação;
- Teste não anunciado – Teste sem agendamento, ou teste surpresa, para simular a recuperação das operações no CPD de recuperação;

- Exercício estratégico – Simulação de recuperação realizado num ambiente paralelo.

Para não afetar o normal funcionamento da empresa os testes são realizados seguindo a ordem seguinte:

- Realização de um caminho estruturado em papel logo que a evolução do plano de continuidade se encontre completo;
- Realização de um exercício estratégico que permite verificar se todos os membros da equipa percebem as suas responsabilidades e condições;
- Realização de um teste de recuperação, agendado, no qual seja necessário a ativação simulada da totalidade do sistema operativo, assim como, dos produtos e de todas as aplicações críticas. Este teste abrange as exigências básicas e não tem a participação de utilizadores;
- Realização de um teste de recuperação, agendado, para ativar a totalidade do sistema operativo e das aplicações críticas. Este teste tem a participação, no mínimo, de um utilizador por cada aplicação critica no CPD de recuperação. Verificação da comunicação de dados e se a mesma se encontra disponível e pode ser ativa;
- Realização de um teste de recuperação, agendado, para ativação da totalidade do sistema operativo e das aplicações a recuperar. Este teste tem a participação, no mínimo, de um utilizador por cada aplicação critica no centro de recuperação. Deve ser selecionada alguma comunicação de dados para ser testada e ligada para verificação.
- Realização de um teste de recuperação, não agendado, para a execução do plano de continuidade e a ativação da totalidade das comunicações. Este teste envolve utilizadores para verificar se a recuperação foi completa, assim como, devem ser realizadas operações paralelas com o CPD;

Todos os planos de teste devem ser estruturados previamente, ao longo do teste é necessário o registo detalhado dos problemas encontrados.

Panoramas de teste incluídos pelo plano de teste da organização:

- Testar a capacidade de flexibilidade a falhas de energia elétrica – Autonomia e plano de ação para colmatar a possibilidade de ausência de autonomia;
- Testar a capacidade de recuperação perante a indisponibilidade de um sistema CORE – Perda de dados ou indisponibilidade de um dos CPDs;
- Testar a capacidade de recuperação perante a indisponibilidade de uma, ou mais áreas, de trabalho;
- Testar a capacidade de recuperação perante a indisponibilidade das comunicações de dados e voz;
- Testar a capacidade de recuperação perante indisponibilidade de um fornecedor crítico;
- Testar a capacidade de recuperação perante indisponibilidade de recursos humanos;
- Testar a capacidade de recuperação perante indisponibilidade dos dois CPDs ou dos três edifícios.

O Plano de Teste deve incluir os seguintes elementos:

- Critérios do teste dos participantes envolvidos
  - Plano de notificações, software e sistema a testar.

- Finalidade do teste
  - Catalogar finalidades primárias e secundárias do teste e resultados esperados.

- Lista de tarefas
  - Selecionar e fundamentar as tarefas a serem realizadas;
  - Instituir tempo de início e de conclusão por atividade.

- Avaliações e medições do teste
  - Registo do horário de início e término das atividades;
  - Validação dos dados recuperados;
  - Descrição documentada dos problemas encontrados;
  - Registo dos desvios sobre o plano de teste.

- Revisão das questões que se seguem
  - Os critérios encontravam-se corretos?
  - As finalidades foram alcançadas?
  - Os critérios de medição estavam certos?
  - Quais as áreas com problemas e quais os aspetos positivos e desvios do plano?
  - Quais as recomendações a apontar para melhorias?

4.6.2. **Plano de Concretização de Testes**

O plano de concretização de testes contém 13 testes divididos por 169 controlos e incluem a totalidade dos componentes críticos da infraestrutura, nomeadamente:

- Teste sobre a eficácia de tolerância a quebras de energia elétrica;
- Teste sobre a eficácia de recuperação perante a indisponibilidade de um sistema CORE;
- Teste sobre a eficácia de recuperação perante a indisponibilidade de um dos CPDs;
- Teste sobre a eficácia de recuperação perante indisponibilidade ou corrupção de dados;
- Teste sobre a eficácia de recuperação perante indisponibilidade de uma ou mais áreas de trabalho;
- Teste sobre a eficácia de recuperação perante indisponibilidade das comunicações de voz;
- Teste sobre a eficácia de recuperação perante indisponibilidade das comunicações de dados;
- Teste sobre a eficácia de recuperação perante indisponibilidade de um fornecedor critico;
- Teste sobre a eficácia de recuperação perante indisponibilidade de recursos humanos;
- Teste sobre a eficácia de recuperação perante indisponibilidade dos três edifícios sede;
- Teste sobre a eficácia do plano de comunicação;
- Teste sobre a eficácia de evacuação;
- Teste sobre a eficácia de ativação do Plano de Gestão de Crise.

Relativamente ao plano de concretização de testes completo de ativação do CPD de recuperação, este ocorreu pela última vez na empresa em 2013 e teve 98,8% de taxa de sucesso na totalidade dos controlos definidos.

4.7. **MONITORIZAÇÃO – SISTEMA AMBIENTAL E SISTEMAS DE SERVIÇOS**

Para abranger a totalidade da infraestrutura foram instalados dois sistemas de monotorização, um ambiental e um de sistemas e serviços, nomeadamente com as seguintes caraterísticas:

- Um sistema de controlo ambiental
  - Vídeo vigilância nos dois CPDs;
  - Detetor de humidade e temperatura no corredor de ar quente e frio;
  - Detetor de inundação instalado debaixo do chão falso;
  - Ligação às UPS de alerta em situação de dano, avaria, ou passagem para a corrente assistida;
  - Ligação e alerta do sistema de deteção de avarias e extinção de incêndio e disparo da extinção;
  - Possibilidade de monitorizar os CPDs de modo central com receção de alertas através de e-mail, se o problema ocorrer fora do horário de expediente o alerta é enviado para a equipa de prevenção de sistemas.

- Um de monitorização de sistemas e serviços
  - Foi instalado o sistema de monitorização *System Center Operations Manager* para colmatar a necessidade de monitorizar os servidores e respetivos serviços, recolher alertas sobre o estado da infraestrutura de servidores;
  - Uma consola central de alarme que usa uma abordagem de *management packs* particulares para cada um dos tipos de serviços, com normas de monitorização que podem ser personalizadas consoante as necessidades, fornecendo alarme, não só para o hardware ou software, mas também, do serviço na sua totalidade;
  - Os diversos serviços podem ser associados como componentes de um serviço global comum, como por exemplo o de uma aplicação web que agrupa os componentes de hardware e software da totalidade dos servidores intervenientes no processo de

disponibilização do serviço tais como: *domain controler;* equipamentos de rede; base de dados; serviços de IIS; balanceadores de carga e uma vista da aplicação na qual o sistema de monitorização simula um utilizador a efetuar uma operação na aplicação medindo a performance da operação e disparando alertas, caso atinja os valores definidos.

As aplicações estabelecidas, tal como o exemplo acima referido, podem estar associadas em serviços provendo uma visão geral.

Outra funcionalidade importante sobre esta ferramenta é a conceção de *dashboards* que apresentam a informação de modo sumário e de fácil leitura aos técnicos de monitorização. Esta ferramenta simplifica, de modo antecipado, a deteção de problemas. Todos os alertas produzidos são recebidos pela equipa de operações e monitorização e são conduzidos para as equipas de prevenção fora do período de trabalho.

5. ANÁLISE E DISCUSSÃO DE RESULTADOS

Com suporte nas normas e práticas investigadas na revisão bibliográfica e após as boas práticas implementadas pela empresa será registada a análise do que foi desenvolvido pela empresa.

Para facilitar a análise e leitura será produzido um código, um sistema de cores, com a seguinte leitura:

Objetivo alcançado – Indica que o objetivo foi cumprido pela empresa;

Objetivo parcialmente alcançado – Indica que o objetivo foi cumprido em parte pela empresa, tendo existido ainda pontos a melhorar;

Objetivo não alcançado – Representa que o objetivo não foi cumprido;

Por fim será calculada a percentagem de conformidade (*compilance)* para cada conjunto de boas práticas implementado na empresa.

5.1 GESTÃO DA CONTINUIDADE DE NEGÓCIO

Tal como foi referido anteriormente na revisão da literatura a gestão da continuidade de negócio abrange toda a organização com a finalidade de identificar ameaças que colocam em causa a continuidade da organização e garantir uma capacidade de resposta eficiente contra as ameaças identificadas. Deste modo permanecem quatro pontos-chave que devem ser considerados na gestão da continuidade de negócio, tais como:

1. Compreender que as necessidades da organização passam pela necessidade de criação de um plano de continuidade de negócio, as suas políticas e os seus objetivos.

   Objetivo alcançado, devido a terem sido observadas todas as áreas e investigados os processos chave e os seus impactos para o negócio.

2. Implantar controlos e métricas para medir a capacidade geral de resposta da organização a incidentes interruptivos.

   Objetivo parcialmente alcançado, devido aos testes periódicos de avaliação da capacidade de recuperação não envolverem todas as áreas da organização, assim como, alguns pontos no plano de teste que não foram testados, tais como a capacidade de recuperação perante a indisponibilidade de recursos humanos que torna necessária uma restruturação de hierarquias. Porém, existe o registo de controlos e métricas, no registo de testes, que podem ser usados para medir a capacidade de resposta da organização a incidentes interruptivos.

3. Supervisionar o funcionamento e a permanência do plano de continuidade de negócio.

   Objetivo parcialmente alcançado, ao longo dos testes periódicos é medido o comportamento e permanência do plano, porém, como já foi referido, nem todos os componentes foram testados apesar do plano de testes referir que a periocidade dos mesmos deve ocorrer anualmente. A data do último teste (2013) comprova claramente a evidência já referida.

4. Melhoramento contínuo fundamentado na avaliação dos objetivos.

   Objetivo alcançado, a documentação que suporta a gestão da continuidade de negócio é revista e atualizada anualmente e mantém a concordância com os objetivos do negócio, considerando os resultados dos testes realizados para a melhoria do processo.

Os objetivos da gestão de continuidade de negócio passam por dois pontos essenciais: a recuperação em caso de interrupção e o valor acrescentado que as boas práticas de gestão de continuidade de negócio alcançam para a organização. Deste modo, podem-se considerar os seguintes objetivos da gestão da continuidade de negócio:

- Proteção do valor da organização beneficiando os acionistas.

  Objetivo alcançado com a preservação do negócio e imagem da organização para o cliente, ampliando a disponibilidade dos sistemas e criando mecanismos de continuidade em caso de desastres do tipo 3.

- Melhoramento da perceção do negócio como consequência da análise de riscos.

  Objetivo alcançado, através do BIA onde são mapeados os processos críticos e os seus impactos para o negócio.

- Recuperação operacional decorrente da redução de risco.

  Objetivo alcançado, por via de arquiteturas de alta disponibilidade e gestão de TI segundo as melhores técnicas identificadas do ITIL.

- Diminuição de *downtime* através da identificação de *workarounds* para abrandar as disrupções.

  Objetivo alcançado, através da redução do *downtime* e inserção de *workarounds* de modo a reduzir as disrupções, sendo que a maioria dos *workarounds* é realizada de modo automático através de tecnologia de alta disponibilidade.

- Conseguem ser identificados assuntos de conformidade para outros processos.

  Objetivo alcançado, devido a tratar-se de uma instituição financeira compreendida por regulamentação do agente regulador (Banco de Portugal) e acordos internacionais como o Basileia III, assim como, foram estimadas as condições impostas pelos regulamentos e convenções.

- Os registos de importância para a organização conseguem ser preservados e protegidos.

  Objetivo alcançado, a totalidade dos registos de importância superior são realizados em formato eletrónico e conservados em áreas restritas. A totalidade da informação considerada critica está compreendida pela política de backup.

- Os assuntos relativos à legislação de saúde e segurança são estimados.

  Objetivo alcançado, foram considerados os assuntos de legislação e regulamentação no desenvolvimento do plano de continuidade da atividade. A implementação dos novos CPD foi desenhada tendo em conta os assuntos de saúde e segurança.

- Melhoramento operacional através da restruturação da engenharia de processos de negócio.

  Objetivo parcialmente alcançado, não existem certezas claras de alterações aos processos de negócio provenientes da gestão de continuidade do negócio, no entanto, os processos de negócio estão constante progresso e podem estar sem sintonia com a gestão da continuidade.

- Defesa dos ativos físicos e da compreensão do negócio.

  Objetivo alcançado, a compreensão e o conhecimento do negócio é salvaguardado através da atualização periódica do BIA, assim como, os ativos físicos, também, estão salvaguardados pelas medidas de segurança realizadas na organização.

- Proteção dos mercados assegurando a continuidade da atividade.

  Objetivo alcançado, assegurar o negócio em situação de risco, ou desastre, contribuí de modo substancial para a proteção do mercado devido à organização constituir um papel importante na empregabilidade e na economia.

- Melhoramento da segurança geral.

  Objetivo alcançado, tanto nas políticas e processos instaurados, como também nos assuntos de saúde e segurança, analisados no planeamento dos CPD, contribuem substancialmente para a melhoria da segurança geral.

Conclui-se claramente, após a análise de gestão da continuidade de negócio que grande parte dos objetivos foram alcançados e a sua prática contribuiu para gerar uma organização com maior resistência e menor vulnerabilidade salvaguardando as vantagens dos seus *stakeholders,* do seu *branding* e da sua corrente de valor.

De qualquer modo, existe margem para melhoramentos na execução do plano de testes que devem ser executados com maior regularidade, realizando a totalidade dos testes e integrando as explicações aprendidas no decurso do processo de negócio.

Nível de Conformidade = 86.6%

5.2. **BIA - *BUSINESS IMPACT ANALYSIS***

Tal como foi referido, anteriormente, na revisão da literatura o processo BIA analisa as principais atividades, os processos e o mapeamento dos eventuais impactos disruptivos referentes ao negócio da organização.

Podem ser referidos três objetivos primordiais a alcançar com o BIA:

- Demarcar os processos críticos e a criticidade de recuperação para o negócio.

  Objetivo parcialmente alcançado, os processos críticos e o seu impacto para o negócio estão bem definidos, porém, a atual versão do BIA não estabelece um nível formal de criticidade, no entanto pode ser investigado através do indicador MTD (*Maximum Tolerable Downtime*) corrente em todos os processos, aplicações e através do RTO e POR estabelecidos.

- Identificação de recursos.

  Objetivo parcialmente alcançado, apesar dos recursos humanos estarem identificados nem todas as áreas referem os recursos de equipamento, de dados e de comunicações.

- Identificar as prioridades de recuperação.

  Objetivo não alcançado, ausência de um registo formal das prioridades de recuperação no BIA, apesar destas prioridades poderem ser acompanhadas pelo MTD mais baixo.

Conclui-se claramente, após a análise do BIA que este se encontra bem estruturado e que incluí a avaliação dos impactos de um desastre para o negócio, porém não foram encontradas provas de uma escala de criticidade para os processos e que nem todas as áreas referem os recursos indispensáveis à recuperação. Não se constata que existe uma escala de prioridades de recuperação.

Nível de Conformidade = 33.3%

5.3. **RECUPERAÇÃO DE DESASTRES (RD) OU *DISASTER RECOVERY (DR)***

Tal como mencionado anteriormente na revisão da literatura, Recuperação de Desastres ou *Disaster Recovery* é a aptidão de uma organização para superar um funcionamento anormal ou uma interrupção do serviço perante um incidente e continuar a prover um serviço após esse incidente.

Objetivo alcançado, devido à criação de uma infraestrutura por parte da organização de alta disponibilidade sustentada em dois CPDs novos, um tier IV principal e um tier II de recuperação, separados pela distância de 20Km. Foi utilizado, para a estrutura de rede, o princípio de alta disponibilidade que utilizou a redundância e caminhos opcionais para todas as ligações externas e entre equipamentos, bem como os princípios da virtualização para os servidores e serviços disponíveis. Através dos testes realizados, a política e processos de gestão de continuidade da atividade foi verificada e apresentou capacidade de recuperação da atividade no CPD de recuperação (respeitando o MTD, RTO e POR definido no BIA).

Nível de Conformidade = 100%

5.4. **ANÁLISE DA NORMA ISO 22301**

Tal como já foi referido anteriormente, a Norma ISO 22301 tem um caráter genérico, internacional, com uma política aplicável a todas as organizações e refere os requisitos específicos para planeamento, revisão e manutenção do processo de continuidade de negócio.

5.4.1. **Contexto da Organização**

Tendo em conta o contexto e os objetivos estratégicos do negócio (produtos e serviços chave, flexibilidade ao risco e obrigações legais e regulatórias) referente à organização é neste ponto de vista necessário reconhecer o campo de ação do PCN.

A organização, dentro do seu contexto, deve criar competências através de um documento com os seguintes elementos:

- Criar uma identificação das atividades, funções, serviços, fornecedores, produtos e parcerias. Distinguir o impacto para estas atividades caso ocorra um incidente disruptivo.

  Objetivo alcançado através de uma identificação das atividades, funções, serviços, fornecedores, produtos e parcerias e o referente impacto BIA.

- Criar pontos de ligação entre as estratégias de continuidade do negócio e os objetivos e políticas da organização que incluam as estratégias de risco gerais.

  Objetivo parcialmente alcançado devido a não existirem provas claras de um documento regulador com a estratégia de risco geral, porém o PCN disposto em conformidade com os objetivos da organização.

- Apetência ao risco da organização.

  Objetivo não alcançado devido a não existirem evidências de um registo da propensão ao risco.

- Relacionar de modo articulado os objetivos da organização com o plano de continuidade de negócio.

  Objetivo alcançado através do alinhamento entre os objetivos da organização e os objetivos do PCN.

- Determinar as causas internas e externas que estimulam o risco.

  Objetivo não alcançado devido ao documento que descreve o plano de gestão de crise, no qual é indicado o tipo de desastres, não distinguir os fatores potencializadores do risco.

- Determinar o critério de risco levando em consideração a propensão da organização ao risco.

  Objetivo não alcançado devido a não existirem registos de propensão ao risco.

- Determinar o objetivo do PCN.

  Objetivo alcançado, o objetivo do PCN está determinado no modelo de gestão do PCN.

- A totalidade das partes envolvidas no PCN.

  Objetivo alcançado devido à envolvência da totalidade das partes envolvidas no PCN.

- As exigências da totalidade dos interessados.

  Objetivo alcançado devido à realização do levantamento de exigências que é mantido atualizado no BIA.

A organização deve definir no documento os seguintes setores:

- Definir as áreas da organização que devem estar incluídas no PCN.

  Objetivo alcançado, as áreas foram incluídas e descritas no Plano de Gestão de Crise do PCN.

- Instituir as exigências do PCN, fundamentando a missão, os objetivos e os deveres internos e externos da organização.

  Objetivo alcançado, as exigências foram definidas no BIA para a missão, para os objetivos e para os deveres internos e externos da organização.

- Reconhecer os serviços e os produtos, assim como, todas as atividades relacionadas com o contexto do PCN.

  Objetivo alcançado, tanto os serviços como todas as atividades que os sustentam foram definidas no BIA.

- Reconhecer as carências e interesses de todas as partes envolvidas (investidores, clientes, fornecedores, acionistas, comunidade e expetativas dos interessados).

  Objetivo alcançado, devido a terem sido considerados os interesses dos envolvidos no desenvolvimento do plano do PCN.

- Determinar, a natureza, o tamanho e a complexidade da organização no contexto do PCN.

  Objetivo não alcançado, não foi determinado, formalmente, no contexto do PCN.

Não foi realizado um documento para determinar, formalmente, o contexto do PCN, porém, foram desenvolvidos alguns parâmetros analisados em outros documentos do PCN.

Não foram encontradas provas claras, na totalidade da documentação, sobre um documento que abrangesse a informação atualizada legalmente. Deve ser desenvolvido e mantido atualizado um documento com as caraterísticas legais, (existe um parecer do Banco de Portugal

sobre planos de continuidade da atividade), que regulam a atividade da organização referente à continuidade da atividade, das operações, produtos e serviços.

Nível de Conformidade = 67.8%

5.4.2. **A Liderança e o Papel da Gestão**

A liderança e o compromisso, com o PCN, devem ser demonstrados a partir da gestão de topo que deve ser responsável pelas seguintes ações:

- Garantir que o PCN é conciliável com a estratégia da organização.

  Objetivo alcançado devido à gestão de topo participar na comissão de crise responsável pela definição e manutenção do PCN.

- Incluir as condições do PCN nos procedimentos da empresa.

  Objetivo alcançado devido a terem sido incluídas as condições do PCN nos procedimentos da empresa.

- Possibilitar os recursos necessários.

  Objetivo alcançado, foram cedidos os recursos necessários à definição e implementação do PCN.

- Informar sobre a importância do PCN.

  Objetivo parcialmente alcançado, o PCN acompanha o desenho de soluções novas, ou de novos serviços, no entanto, não existe uma informação institucional para fortalecer a relevância do PCN.

- Garantir que o PCN atinge os efeitos aguardados.

  Objetivo alcançado, foi realizado, com frequência, um acompanhamento dos testes ao PCN.

- Orientar e sustentar o processo de continuidade da melhoria.

  Objetivo alcançado através da participação de membros da comissão de crise que apoiam a continuidade da melhoria do processo.

- Instituir e transmitir a política de continuidade de negócio.

  Objetivo não alcançado devido à política de continuidade estar inserida no modelo de gestão do PCN.

- Garantir que o planeamento e os objetivos do PCN são realizados.

  Objetivo alcançado devido à existência de um regular acompanhamento do planeamento e objetivos de realização do PCN.

- Garantir que as obrigações dos papeis principais são conferidas.

  Objetivo alcançado, a comissão de crise conferiu responsabilidades e papeis na concretização do PCN.

- Dirigir e apoiar os recursos humanos envolvidos com o PCN.

  Objetivo alcançado devido à participação da comissão de crise e do seu acompanhamento aos testes cíclicos.

- Proteger outras áreas de gestão exemplificando liderança e compromisso com o PCN.

  Objetivo alcançado devido à exemplificação do compromisso da gestão de topo, com o PCN, no apoio a outras áreas de gestão, sempre que necessário.

- Determinar as regras de concordância para os riscos e determinar quais os níveis de risco aceitáveis.

  Objetivo não alcançado não existem certezas claras sobre a definição de critérios de risco.

- Participação e transmissão ativa nos testes.

  Objetivo alcançado devido à participação e apoio nos testes realçando a importância dos mesmos junto de todas as áreas de negócio.

- Garantir a realização de auditorias ao PCN.

  Objetivo não alcançado, não são realizadas auditorias ao PCN.

- A política deve ser adequada à atividade da organização.

  Objetivo não alcançado, a política está inserida no documento Manual de Gestão do PCN e não existe um documento independente sobre a mesma, porém a política é adequada à organização.

- A política deve esclarecer sobre o modo de trabalho, ou moldes de trabalho, para definir os objetivos da continuidade de negócio.

  Objetivo não alcançado, não existe o esclarecimento sobre os moldes de trabalho para definir os objetivos da continuidade de negócio, porém o molde de trabalho para atingir os objetivos está acessível em todos os documentos que o objetivo principal é recuperar a atividade em caso de desastre.

- Os requisitos definidos devem ser satisfeitos através da política.

  Objetivo não alcançado, a política está inserida no documento Manual de Gestão do PCN.

- A política deve incentivar uma melhoria contínua do PCN.

  Objetivo não alcançado, a política não incentiva a melhorias continuas do PCN.

A política do PCN deve compreender as seguintes caraterísticas:

- O documento deve estar sempre disponível.

  Objetivo não alcançado devido ao documento sobre a política estar incorporado no documento Manual de Gestão do PCN e por esse motivo não é um documento independente e não está sempre acessível como documento.

- A política do PCN deve ser comunicada à organização e estar disponível a todas as partes interessadas.

  Objetivo não alcançado, a política do PCN está inserida no documento Manual de Gestão do PCN e não está disponível a todas as partes interessadas

- Deve ser inspecionada e atualizada em pequenos intervalos de tempo, ou caso exista alguma modificação considerável.

  Objetivo não alcançado devido à última atualização, ou modificação, ter ocorrido à mais de um ano.

Após a análise do último ponto é possível concluir, de modo sucinto, que a gestão de topo está incluída no PCN, porém não tem um documento formal individual sobre a política de continuidade da atividade, devido à mesma estar inserida no mesmo documento do Manual de Gestão do PCN que não tem uma atualização à cerca de um ano.

Nível de Conformidade = 52.3%

5.4.3. **Planeamento**

No desenvolvimento do planeamento é necessário considerar os pontos já referidos anteriormente. O planeamento deve assegurar os seguintes elementos:

- Garantir que consegue assegurar os objetivos que foram nomeados.

Objetivo alcançado, os objetivos de recuperação nomeados são passíveis de serem alcançados.

- Precaver ou restringir resultados indesejados.

Objetivo alcançado, o planeamento foi realizado com o objetivo de evitar resultados indesejados.

- Alcançar uma continuidade na melhoria.

Objetivo alcançado, existe uma revisão dos documentos para manter a continuidade na melhoria dos mesmos com frequência.

A organização deve planificar:

- As condutas para dirigir os riscos e as oportunidades.

Objetivo alcançado, são reconhecidos os riscos e as oportunidades e as condutas são planificadas de modo a reduzir os riscos.

- Incluir e executar as ações no processo de continuidade de negócio.

Objetivo alcançado, as ações de redução de riscos são incluídas no processo.

- Estimar a aplicação dessas ações.

Objetivo alcançado, na realização dos testes são estimados os resultados das ações.

Os objetivos devem:

- Ter consistência com a política de continuidade de negócio.

Objetivo alcançado, os objetivos têm consistência com a política de continuidade de negócio.

- Considerar o nível mínimo de serviço/produção que é concebível para a organização.

Objetivo alcançado, os objetivos estabelecidos no BIA levam em consideração os níveis mínimos de serviço/produção que é concebível para a organização.

- Ser apreciáveis.

Objetivo alcançado, os objetivos de recuperação são concretos e apreciáveis.

- Ter em consideração as condições definidas.

Objetivo alcançado, os objetivos têm em consideração as condições definidas no BIA.

- Serem supervisionados e atualizados.

Objetivo alcançado, os objetivos são atualizados com frequência no BIA.

A organização deve sustentar os objetivos fundamentados para produzir o documento de objetivos da continuidade da atividade, que deve determinar:

- Delinear o responsável.

Objetivo não alcançado, não existe claramente um documento formal de objetivos, ainda que os mesmos sejam traçados no BIA.

- O que vai ser realizado.

Objetivo não alcançado, inexistência de um documento formal de objetivos, ainda que os mesmos sejam traçados no BIA.

- Quais os meios ou recursos necessários.

Objetivo não alcançado, o documento formal de objetivos não existe, apesar dos objetivos serem descritos no BIA.

- Quando ficará finalizado e completo.

Objetivo não alcançado, o documento formal de objetivos não existe, apesar dos objetivos serem descritos no BIA.

- Qual o modo de avaliação dos resultados.

  Objetivo não alcançado, o documento formal de objetivos não existe, apesar dos objetivos serem descritos no BIA.

  A organização realizou o planeamento para a recuperação da atividade, porém não existe um documento formal de objetivos, apesar dos objetivos serem descritos no BIA. Recomenda-se a criação formal do documento em causa.

  Nível de Conformidade = 68.7%

5.4.4. **Suporte do PCN**

A base de eficiência do PCN está apoiada na utilização de recursos adequados para cada tarefa. É importante garantir a formação adequada dos recursos humanos e da comunicação.

A organização deve demarcar e prover os recursos necessários para a criação, implementação, manutenção para a melhoria continua do PCN, para tal a organização deve:

- Demarcar as aptidões necessárias dos recursos humanos que irão executar o PCN.

  Objetivo parcialmente alcançado, não existem referências sobre as competências no PCN, embora o plano de gestão da crise faça referências a funções de modo implícito referindo que determinada função possui determinadas competências.

- Garantir que os recursos humanos são competentes e possuem a formação, educação e experiência apropriada.

  Objetivo parcialmente alcançado, na contratação dos recursos humanos são verificadas referências como a formação, educação e experiência.

- Quando apropriado tomar ações de modo a obter competências e avaliar o resultado dessas ações.

  Objetivo não alcançado, não existem provas de ações com o objetivo de aumentar as competências pretendidas.

- Preservar os documentos adequados para prova das competências.

Objetivo não alcançado, não é preservado um registo de provas das competências na documentação do PCN.

Os recursos humanos que intervêm no PCN devem possuir conhecimento:

- Sobre a política de continuidade de negócio.

Objetivo alcançado, é disponibilizada a documentação a todos os recursos humanos que intervêm no PCN.

- Sobre o seu papel e o seu contributo para o PCN.

Objetivo alcançado, os recursos humanos intervenientes no PCN têm conhecimento do seu papel e do seu contributo.

- Sobre as implicações de não seguir o PCN.

Objetivo alcançado, os recursos humanos intervenientes no PCN têm conhecimento das implicações de não seguir o PCN.

- Sobre o seu papel em caso de acidente disruptivo.

Objetivo alcançado, os recursos humanos intervenientes no PCN têm conhecimento em caso de acidente disruptivo.

A organização deve delinear a comunicação interna e externa, abrangendo:

- O que deve e o que não deve ser comunicado.

Objetivo alcançado, o Plano de Gestão de Crise traça e descreve o que deve ser comunicado.

- Quando deve ser comunicado.

Objetivo alcançado, o Plano de Gestão de Crise traça e descreve quando comunicar.

- A quem deve ser comunicado.

Objetivo alcançado, o Plano de Gestão de Crise traça e descreve a quem comunicar.

A organização deve executar, manter e atualizar um procedimento para:

- Comunicar internamente aos recursos humanos envolvidos da organização.

Objetivo alcançado, o Plano de Gestão de Crise traça e descreve a conduta de comunicação interna.

- Comunicar externamente aos clientes, parceiros, comunidade envolvente e aos média.

Objetivo alcançado, o Plano de Gestão de Crise traça e descreve a conduta de comunicação externa e para a comunicação social.

- Fundamentar, receber e responder a comunicações das partes envolvidas.

Objetivo não alcançado, não existem documentos que comprovem o procedimento de fundamentar, receber e responder a comunicações das partes envolvidas.

- Adequar um conjunto de alertas de ameaças regionais e nacionais.

Objetivo não alcançado, a organização não adequou um conjunto de alertas.

- Garantir a continuidade dos meios de comunicação durante um evento interruptivo.

Objetivo alcançado, está garantida a continuidade dos meios de comunicação durante um evento interruptivo.

- Transmissão às autoridades.

Objetivo não alcançado, o documento relativo ao Plano de gestão de Crise, nos seus procedimentos de comunicação, não contempla a transmissão às autoridades.

- Execução de testes ao plano de comunicação a utilizar durante um evento interruptivo.

Objetivo alcançado, o plano de execução de testes refere um teste efetuado com sucesso no plano de comunicação.

O PCN deve envolver os seguintes aspetos:

- Documentação mencionada nesta ISO.

Objetivo não alcançado, alguns documentos na ISO não foram incluídos no PCN da organização.

- Os documentos, considerados importantes para o sucesso do PCN, podem ter variantes.

Objetivo alcançado, existem documentos acessórios no PCN da organização.

Na conceção do documento a organização deve garantir os seguintes elementos:

- A identificação e descrição do documento (data, autor, título e número de referência), o formato (versão, software e linguagem entre outros elementos que podem ser considerados necessários) e media (papel, formato eletrónico, entre outros).

Objetivo alcançado, os documentos estão corretamente identificados e também existe em formato eletrónico.

Os documentos devem ser verificados para garantir os seguintes procedimentos:

- A sua disponibilidade e a sua proteção apropriada (confidencialidade, integridade e perda de informação).

Objetivo alcançado, os documentos estão configurados eletronicamente e devidamente protegidos a acessos não autorizados (com backups frequentes).

Para verificar a informação relativa ao documento a organização deve realizar as seguintes atividades sempre que seja necessário aplicar as mesmas:

- Recuperação, distribuição, preservação, acesso, utilização e controlo de alterações.

  Objetivo alcançado, os documentos estão em configurados e protegidos eletronicamente contra acessos não autorizados e disponíveis a todos os envolvidos (com backups frequentes). A documentação mantém um histórico de versões e modificações.

- Conservação da sua legibilidade (documento de leitura clara) e preservação de utilização de informação caduca.

  Objetivo alcançado, a documentação tem clara legibilidade, a documentação caduca é retirada e mantida numa pasta de histórico mantendo deste modo a documentação disponível sempre atualizada.

Relativamente à análise de suporte a organização tem os meios de controlo e comunicação necessários, porém não existe a gestão de competências no PCN. O plano de comunicações deve ser melhorado para abranger as comunicações com as autoridades e deve incluir a uma conduta de receção, registo e resposta relativamente a comunicações externas. Tal como já foi referido anteriormente a organização não detém a totalidade dos documentos descritos na ISO 22301.

Nível de Conformidade = 76.6%

5.4.5. **Operacionalização/Execução**

Esta etapa abrange a execução do planeamento realizado nos pontos antecedentes. A organização deve planear, executar e controlar o processo do seguinte modo:

- Instituir um critério para os processos, implementar um mecanismo de controlo de processos baseado nos critérios definidos.

  Objetivo alcançado, foi instituído um critério definido no modelo de gestão do PCN e existe um mecanismo de controlo definido pelo modelo de gestão do PCN.

- Manter um registo atualizado para garantir que os processos vão sendo executados mediante o que foi estabelecido.

  Objetivo parcialmente alcançado, o único registo de execução está contido no plano de execução de testes.

A organização deve implementar e preservar um processo protocolar e documentado para o *business impact analysis and risk assessment* do seguinte modo:

- Instituir o contexto de avaliação, definir critérios e a avaliação do impacto potencial do evento interruptivo.

  Objetivo alcançado, apesar do BIA conter o potencial impacto de um evento interruptivo para o processo de negócio, porém não estabelece o critério e o contexto.

- Levar em consideração os requisitos legais e outros considerados relevantes pela organização.

  Objetivo alcançado, foram levados em consideração a totalidade dos aspetos relevantes para a organização.

- Incluir uma análise organizada e frequente com prioridade de tratamento do risco e da sua relação de custos.

  Objetivo parcialmente alcançado, não incluí a prioridade do tratamento de risco, embora contemple a sua relação de custos em alguns processos.

- Clarificar as condições de output do business *impact analysis and risk assessment*.

  Objetivo alcançado, foram clarificados com sucesso os outputs.

- Particularizar as condições nas quais a informação é atualizada e confidencial.

  Objetivo parcialmente alcançado, existem condições de atualização, no entanto não existem condições no que refere à confidencialidade.

O BIA deve incluir os procedimentos seguintes:

- Reconhecer atividades que suportam o negócio e avaliar as colisões nas atividades ao longo do tempo.

Objetivo alcançado, foram reconhecidas as atividades que suportam o negócio e foram avaliadas as colisões para todas as atividades ao longo do tempo.

- Demarcar prazos, máximos e mínimos, para voltar às diferentes atividades dentro de um nível mínimo admissível tendo em vista um prazo máximo a partir do qual não é admissível para o negócio. Reconhecer os recursos vitais para as atividades abrangendo outras partes relevantes tais como parceiros e fornecedores.

Objetivo alcançado, existe um prazo máximo estabelecido para todas as atividades e estão admitidos os recursos vitais para todas as atividades incluindo todas as partes relevantes.

A organização deve gerar e manter um processo de avaliação de riscos oficialmente documentado, que, de modo frequente, reconheça analise e avalie o risco de eventos interruptivos para a organização, tendo em conta a seguinte informação:

- Reconhecer os riscos de eventos interruptivos para as atividades, sistemas, informação, processos, pessoas, parceiros e bens entre outros recursos que os suportem.

Objetivo alcançado, o Plano de Gestão de crise reconhece os riscos para a atividade.

- Observar os riscos de modo contínuo e sistemático. Avaliar quais os eventos interruptivos que requerem intervenção.

Objetivo não alcançado, não existem provas de uma análise contínua e sistemática dos riscos e não existe uma avaliação de quais os eventos interruptivos que requerem intervenção.

- Reconhecer os atos conciliáveis com os objetivos de continuidade de negócio e a propensão da organização pelo risco.

Objetivo não alcançado, não existe um reconhecimento da propensão da organização pelo risco.

O método de continuidade do negócio deve fundamentar-se nos outputs do *business impact analysis and risk assessment e* a organização deve demarcar a estratégia adequada para:

- Defender as atividades com maior relevância para o negócio. Retomar as atividades priorizadas e as suas dependências, suportes e recursos. Amenizar, respondendo e administrando os impactos.

  Objetivo alcançado, o PCN foi realizado com suporte nos requisitos do BIA de modo a defender as atividades com maior relevância, crítica, do negócio. O PCN inclui processos de continuidades das atividades críticas e suas dependências definidas no BIA. O PCN abrange planos de amenização dos impactos, restabelecendo a atividade no CPD de recuperação e através de processos manuais.

A organização demarca as condições e recursos para implementar as estratégias selecionadas, os tipos de recursos a observar devem ser os seguintes:

- Pessoas, informação e dados, edifícios, ambiente de trabalho, instalações, equipamento e consumíveis, sistemas e tecnologias de informação e comunicação.

Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.

- Transporte, budget, parceiros e fornecedores.

Objetivo alcançado, o transporte está identificado no Plano de Gestão de Crise como um tipo de recurso. O budget tem um documento acessório com os custos da implementação da solução e os custos mensais estão refletidos no budget da organização. Os parceiros e fornecedores estão identificado no BIA para todos os processos de negócio.

Para tratar dos riscos identificados as organizações devem considerar as seguintes medidas:

- Diminuir a probabilidade de interrupção, diminuir o período de interrupção e limitar o impacto das interrupções nos serviços e produtos base da organização.

  Objetivo alcançado, a probabilidade de interrupção é reduzida através de tecnologias de alta disponibilidade e processos de suporte e manutenção. A existência de uma estrutura

de suporte que inclui equipas de prevenção que atuam diretamente em caso de interrupção. O impacto é limitado através de tecnologias de alta disponibilidade e redundância de sistemas de suporte às aplicações de negócio.

Para gerir os acontecimentos interruptivos e continuar com as atividades de negócio com suporte nos objetivos de recuperação identificados no BIA a organização deve criar, implementar e manter procedimentos de continuidade da atividade com os seguintes procedimentos:

- Instituir protocolos de comunicação internos e externos, clarificar os passos necessários para retomar a atividade em caso de interrupção.

   Objetivo alcançado, o plano de gestão de crise refere o protocolo de comunicação. Existe um documento de suporte com as ações necessárias para restaurar o serviço no CPD alternativo.

- Flexibilidade na resposta a ameaças imprevistas e/ou mudanças das condições internas e externas. Manter o foco no impacto dos eventos interruptivos.

   Objetivo alcançado, os procedimentos são flexíveis. Os procedimentos são focados nos impactos dos incidentes interruptivos.

- Desenvolver com base em probabilidades estabelecidas e na análise de correlações. Eficácia na minimização de consequências através de estratégias de atenuação adequadas.

   Objetivo alcançado, os procedimentos têm em relevância as correlações investigadas no BIA. Os procedimentos são eficazes e testados periodicamente.

A organização deve documentar e executar procedimentos e uma estrutura para responder a acidentes interruptivos através de recursos humanos com autoridade e competência para exercer essa responsabilidade de gerir acidentes e interrupções. Esta estrutura de resposta deve realizar as seguintes atividades:

- Reconhecer o *threshold* para que se justifique o início da resposta formal. Avaliar a extensão e a essência do incidente interruptivo, assim como, o seu possível impacto. Ativar de modo apropriado a resposta de continuidade de negócio.

  Objetivo alcançado, o plano de gestão de crise remete as três informações acima referidas.

- Possuir procedimentos e processos para ativação, operação, coordenação e comunicação. Possuir recursos disponíveis para sustentar o processo e os procedimentos de gestão de incidentes interruptivos de modo a diminuir o impacto dos mesmos.

  Objetivo alcançado, existem procedimentos para cada uma das fases do processo, tais como: lançamento, decisão, ativação, execução, recomeço e recuperação assim como existem recursos para suportar o processo.

- Comunicar externamente com as partes envolvidas, tais como: as autoridades e a média.

  Objetivo parcialmente alcançado, embora exista o procedimento de comunicação o mesmo não contempla a comunicação com as autoridades.

Devem estar contemplados os seguintes procedimentos para:

- Detetar um incidente e monitorizar um incidente.

  Objetivo alcançado, existe um processo de gestão de incidentes, responsável por detetar incidentes interruptivos e também existe um processo de gestão de incidentes que é responsável por monitorizar os mesmos inclusive através de um comité de crise que acompanha a evolução do incidente interruptivo.

- Comunicação interna com a organização documentada.

  Objetivo alcançado, existe procedimento para a comunicação interna no plano de gestão de crise.

- Comunicação externa documentada com as entidades nacionais e/ou regionais de alerta e aviso de riscos.

  Objetivo não alcançado, não existe procedimento de comunicação externa com entidades de aviso de riscos.

- Garantir os meios de comunicação durante um incidente interruptivo.

  Objetivo alcançado, estão calculados os meios de comunicação em caso de acidente interruptivo.

- Organização definida de comunicação externa com as entidades de emergência.

  Objetivo não alcançado, não existe procedimento de comunicação externa com as entidades de emergência.

- Registo de informação crucial sobre o incidente, as ações e as decisões tomadas.

  Objetivo alcançado, existe uma previsão de todas as ações realizadas e informação crucial do incidente.

  A organização deve estabelecer o modo de proceder documentado de respostas a incidentes interruptivos e de como recuperar as atividades lesadas num espaço de tempo pré-definido e deve sobrescrever os requisitos dos recursos humanos que o vão realizar, assim como o PCN deve: definir as responsabilidades atribuídas à equipa de recursos humanos que detém autoridade durante o incidente.

- Definir um processo para ativar a resposta.

  Objetivo alcançado, existe um processo definido no Plano de Gestão de Crise e no plano de recuperação de sistemas.

- Detalhar como gerir as consequências imediatas de um incidente: o bem-estar os indivíduos.

  Objetivo não alcançado, não foram encontradas na documentação medidas reservadas ao bem-estar dos indivíduos.

- Estratégia e opções operacionais de resposta ao incidente.

  Objetivo alcançado, existe um processo definido no Plano de Gestão de Crise e no plano de recuperação de sistemas.

- Detalhar como e em que circunstancias a organização irá comunicar com os funcionários. Como a organização recuperará as suas atividades primordiais dentro do tempo e período definido. Pormenores sobre o modo como a organização deve responder à comunicação social após um incidente.

  Objetivo alcançado, determinado no plano de gestão de crise.

Cada plano deve definir os seguintes propósitos e âmbitos:

- Objetivos, critérios, procedimentos de ativação e procedimentos de implementação.

  Objetivo alcançado, os planos referem os seus objetivos, o plano de gestão de crise estabelece os critérios de ativação dos planos do PCN e também referem os procedimentos de implementação.

- Papéis, responsabilidades e autoridades, procedimentos e requisitos de comunicação.

  Objetivo alcançado, o plano de gestão de crise estabelece os papéis e responsabilidades e também estabelece os requisitos de comunicação.

- Correlações e interdependências internas e externas, requisitos e recursos e fluxo de informação e processos de documentação.

  Objetivo parcialmente alcançado, nem todos os planos referem as interdependências, os recursos e o fluxo de informação e processos de documentação devidamente definidos.

- Após as medidas temporárias aplicadas depois de um incidente de modo a recuperar o seu funcionamento normal a organização deve ter documentadas as atuações de *restore* e recuperação da atividade.

Objetivo alcançado, o plano de recuperação estabelece as atuações do período de recuperação.

- A organização deve realizar testes com regularidade aos procedimentos de continuidade de negócio de forma a garantir o seu alinhamento com os objetivos definidos.

Objetivo alcançado, são realizados testes com regularidade.

A organização deve diligenciar testes que:

- Sejam sólidos e no âmbito do PCN, sejam baseados em cenários adequados, bem planeados, com objetivos bem definidos e realizados ao longo do tempo, validando juntos o plano num todo, devem envolver as partes interessadas.

Objetivo alcançado, os testes descritos no plano de teste são sólidos com o âmbito do PCN, os cenários são adequados e com objetivos definidos, os testes estão distribuídos em blocos que, no seu conjunto, validam o plano na totalidade.

- Devem minimizar o risco de interrupções na atividade normal. Os testes devem de ser corrigidos num processo de melhoria continua.

Objetivo alcançado, os testes estão divididos em blocos de forma a possibilitar os testes das partes sem afetar a totalidade. Os testes são corrigidos a cada execução.

- Devem gerar relatórios com os resultados, advertências e ações para executar melhorias possíveis.

Objetivo não alcançado, não existem provas de relatórios formais com advertências e ações de implementação.

- Os testes devem ser realizados em intervalos planificados, ou sempre que existam alterações consideráveis na organização ou no ambiente onde atua.

Objetivo parcialmente alcançado, a planificação de testes refere que os testes devem ser realizados anualmente, porém já passou mais de um ano desde que foram efetuados os últimos testes.

Pode concluir-se que a organização está pronta para sustentar o PCN, porém existe margem para melhorar o BIA de modo a cumprir todos os requisitos do ISO. As provas insinuam que os documentos do PCN não são atualizados com uma assiduidade definida e que não existe uma análise de riscos realizada de modo sistemático. As atuações de comunicação precisam de ser inspecionadas de modo a contemplar os requisitos da ISO. Não existem relatórios formais sobre os testes com advertências que podem proporcionar melhorias. Para finalizar os testes não respeitam a frequência definida.

Nível de Conformidade = 83.6%

5.4.6. **Análise da performance**

Depois da implementação do PCN a norma ISO 22301 refere a importância de existir uma monotorização estável e permanente e testes frequentes.

Deste modo a organização deve demarcar:

- O que deve ser monitorizado e medido. Os métodos de monitorização, medida, análise e avaliação, de forma a assegurar resultados válidos. Quando a medição e a monitorização devem ser realizadas.

  Objetivo parcialmente alcançado, a única monitorização está indicada no plano de execução de testes. O plano de teste referência a medida de avaliação, mas não menciona os métodos de monitorização e avaliação. A única monitorização está mencionada no plano de execução de testes e são efetuados aquando da execução dos testes.

- Quando é que os resultados da monitorização devem ser avaliados.

  Objetivo não alcançado, não existe na documentação alusão à monitorização, à análise e avaliação.

A organização deve:

- Tomar uma ação, sempre que se justifique necessária, para remeter os resultados antes que suceda uma não conformidade. Guardar toda a documentação sirva de evidência.

  Objetivo não alcançado, não existem provas claras de ações tomadas para remeter resultados antes que suceda uma não conformidade. Os documentos que servem de evidência não são todos guardados.

As condutas de monitorização devem prover:

- Um conjunto de metrificações adequadas à organização.

  Objetivo não alcançado, não existe uma ação formal de monitorização.

- Monitorizar o PCN e o cumprimento dos seus objetivos.

  Objetivo parcialmente alcançado, não existe uma ação de monitorização, no entanto existe um acompanhamento do processo e teste por parte do comité de crise.

- Apontadores de performance dos processos e funções que protegem as atividades prioritárias. Monitorizar a correspondência dos objetivos de continuidade de negócio com a ISO 22301.

  Objetivo não alcançado, não existem apontadores de performance dos processos e funções definidos. Não existe um processo de monitorização em conformidade com a ISO.

- Monitorizar provas históricas de deficiências do PCN.

  Objetivo parcialmente alcançado, é mantido um histórico dos testes, mas não existe uma ação formal de monitorização.

- Proteger os resultados do processo de monitorização e avaliação de modo a simplificar as ações corretivas.

  Objetivo não alcançado, não existe processo formal de monitorização determinado.

Análise e avaliação dos procedimentos do PCN:

- Para garantir o ajuste adequada e a efetividade a organização deve proceder a análises e avaliações aos procedimentos do PCN.

  Objetivo alcançado, os procedimentos são analisados e avaliados de modo periódico.

- As análises e avaliações devem ser realizadas através de revisões periódicas com recurso a testes, relatórios posteriores ao incidente e indicadores de performance. As alterações significativas devem ser refletidas nos procedimentos.

  Objetivo alcançado, são realizadas revisões e testes periódicos e sempre que se justifique são alterados os procedimentos.

- A organização deve analisar periodicamente o cumprimento legal, assim como a aplicação das melhores práticas da indústria em conformidade com os seus objetivos de continuidade de negócio. Deve promover análises periódicas, ou quando exista uma alteração considerável.

  Objetivo alcançado, no processo de revisão periódica é levada em consideração a legislação. Os procedimentos são analisados periodicamente e alterados sempre que existe uma alteração justificada.

A organização deve implementar auditorias internas que devem ser planeadas em intervalos periódicos para analisar o sistema de continuidade de negócio. Averiguar se o sistema de continuidade da atividade está em conformidade com:

- Os requisitos da organização para o PCN. Os requisitos da ISO 22301. Confirmar se o sistema está implementado e é atualizado.

  Objetivo não alcançado, não são realizadas auditorias ao PCN.

A organização deve:

- Planear e implementar um programa de auditoria realizado periodicamente, os seus métodos, responsabilidades, requisitos de planeamento e relatórios. O programa de auditoria deve considerar os resultados das auditorias anteriores. Delimitar os critérios e o âmbito da auditoria. Distinguir os auditores e orientar as auditorias para garantir objetividade e neutralidade ao longo de todo o processo. Garantir que os resultados das

auditorias são cedidos a todos os gestores envolvidos no processo. As provas devem ser guardadas como testemunho da implementação do plano de auditoria.

Objetivo não alcançado, não são realizadas auditorias ao PCN.

Para assegurar que o PCN continua adaptado a gestão de topo deve rever o PCN em períodos pré-estabelecidos. A revisão deve abranger as seguintes apreciações:

- O estado das ações de revisões anteriores. Modificações internas e externas pertinentes para o PCN.

  Objetivo alcançado, as revisões ao PCN levam em consideração as revisões anteriores. As revisões ao PCN levam em consideração as modificações relevantes para o PCN.

- Indicativos de comportamento do PCN, abrangendo não conformidades e ações de correção. Resultados de auditorias.

  Objetivo não alcançado, não existe um plano de auditoria ao PCN.

- Análise e avaliação de resultados sobre o processo de monotorização e avaliação.

  Objetivo parcialmente alcançado, apesar de serem levados em consideração os resultados dos testes ao PCN, não existe um plano de monotorização sobre o mesmo.

- Momentos de melhoria contínua.

  Objetivo alcançado, são levadas em consideração as oportunidades de melhoria contínua.

  A retificação deve considerar a performance da organização abrangendo:

- O acompanhamento de ações de retificação antecipadas. A indispensabilidade de alteração do PCN incluindo política e objetivos. Oportunidade de melhoria.

Objetivo alcançado, existe o acompanhamento das ações de retificação antecipadas. Caso exista necessidade, no processo de retificação periódico, são analisadas e alteradas a política e objetivos. As oportunidades de melhoria são levadas em consideração.

- Resultados de auditorias e retificações ao PCN.

  Objetivo não alcançado, não existe um plano de auditoria ao PCN.

- Procedimentos, técnicas e produtos que poderiam usados, na organização, para melhorar o PCN.

  Objetivo alcançado, nos procedimentos de retificação são analisados os procedimentos, as técnicas e os produtos para melhorar o PCN.

- Situação das ações de correção, resultados dos testes e riscos não dirigidos em conformidade com a avaliação de risco.

  Objetivo alcançado, são analisadas as ações de correção, os resultados dos testes são corrigidos e os riscos verificados na avaliação de risco são analisados e levados em consideração.

- Alterações internas e externas que podem afetar o PCN, confirmar se a política continua adequada e advertências de melhoria.
- Objetivo alcançado, as alterações internas e externas são consideradas no processo de revisão, a política é revista e as advertências de melhoria são consideradas no processo de revisão. Exemplos estudados e ações consequentes de incidentes interruptivos e novas boas práticas.

  Objetivo alcançado, os exemplos estudados com eventos interruptivos são levados em consideração no processo de revisão e as boas práticas, conhecidas pela equipa responsável, também, são levadas em consideração.

Sempre que aplicável, o resultado da revisão deve abranger a tomada de decisões de melhoria continua e as possíveis necessidades de modificação ao PCN do modo que se segue:

- Modificações no campo do PCN, melhorias na eficiência do PCN e atualização da avaliação de risco, BIA, PCN incluindo procedimentos relacionados.

Objetivo alcançado, sempre que se verifique necessário o campo do PCN é revisto e são alterados os procedimentos com o objetivo de melhoramento da eficácia do PCN, assim como, sempre que se justifique são atualizados os referidos procedimentos.

Alteração de procedimentos e fiscalizações que respondem a episódios internos e externos que podem abalar o PCN abrangendo:

Objetivo alcançado, sempre que necessário os procedimentos são modificados para responder a eventos internos e externos que possam abalar o PCN.

- Eficiência de medidas de controlo.

Objetivo alcançado, a equipa de crise revê a eficiência das medidas.

Deve ser arquivada a totalidade da documentação como prova e os resultados obtidos na revisão devem ser comunicados aos interessados, assim como, devem ser tomadas medidas significativas para executar as ações necessárias.

Objetivo não alcançado, devido a não terem sido encontradas provas do processo de revisão para além das modificações executadas.

É possível concluir que os processos e procedimentos são corrigidos de modo periódico, no entanto, a última atualização tenha sido realizada à mais de um ano. Não existem procedimentos de monotorização e não são realizadas auditorias internas de modo periódico, na organização, como indicado na ISO 22301.

Nível de Conformidade = 54%

5.4.7. **Melhoria Contínua**

Pode definir-se melhoria continua como um processo de ações tomadas pela organização para aumentar a eficiência dos processos de modo a alcançar objetivos benéficos para a organização.

Sempre que se verifique inconformidades a organização deve:

- Reconhecer a inconformidade e reagir à inconformidade, assim como, sustentar ações corretivas de forma a excluir a inconformidade.

  Objetivo parcialmente alcançado, as inconformidades são identificadas, porém não existe um procedimento formal para identificar e tratar das mesmas no PCN. São realizadas ações para alterar as inconformidades, porém não existe um procedimento formal de identificação e tratamento dessas inconformidades do PCN.

- Suportar as consequências e avaliar a necessidade das ações com o objetivo de excluir as causas da inconformidade.

  Objetivo alcançado, sempre que se verificam inconformidades as consequências são tratadas.

- Rever e determinar as causas da inconformidade.

  Objetivo parcialmente alcançado, não se verifica a existência de um procedimento no PCN de identificação formal para o tratamento de não conformidades.

- Analisar a existência de inconformidades similares.

  Objetivo não alcançado, não existe uma atuação formal para identificar e tratar as inconformidades do PCN. Não existe um histórico de inconformidades do PCN.

- Analisar a carência de ações de correção para garantir que as inconformidades não se repetem no PCN. Estabelecer e executar as ações corretivas. Revisão da eficiência das ações executadas.

Objetivo parcialmente alcançado, não se verifica a existência de um procedimento formal para identificação e tratamento de inconformidades do PCN. Porém as ações executadas têm como objetivo que a inconformidade não se repita.

- Modificar o PCN, caso se verifique essa necessidade. Executar as ações necessárias.

Objetivo alcançado, sempre que se verifique a necessidade justificada de modificação do PCN o mesmo é alterado. As ações que se destinam a corrigir as inconformidades são realizadas.

- Analise da eficiência das ações corretivas realizadas.

Objetivo parcialmente alcançado, verifica-se que não existe uma atuação formal de identificação e tratamento de inconformidades do PCN.

A organização deve arquivar toda a documentação como evidência clara do seguinte:

- Inconformidades e ações de correção executadas e respetivos resultados dessas ações.

Objetivo não alcançado, verifica-se que não foram claramente encontradas provas das ações corretivas e dos seus respetivos resultados.

Conclui-se que apesar da organização tratar das inconformidades não existe um procedimento sistemático de identificação e tratamento de inconformidades.

Nível de Conformidade = 50%

Depois de analisados os pontos referentes da ISSO 22301 verifica-se que o PCN desenvolvido pela organização ainda terá que desenvolver ações no sentido de atingir um nível de conformidade superior tal como podemos observar na Figura 32, que neste momento situa-se na casa dos 68.3%, entre algumas melhorias está a melhoria do trabalho da gestão que está com um nível de conformidade aproximado de 50%.

Nível de conformidade com ISO 22301 = 68.3%

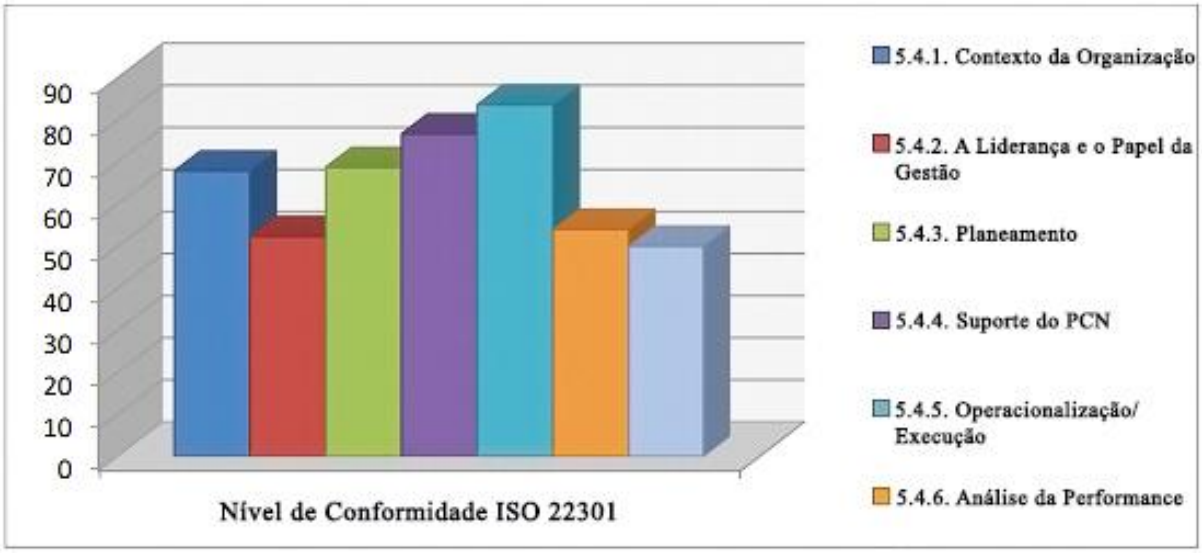


Figura 32: Nível de Conformidade ISO 22301

6. **CONCLUSÃO**

6.1. **CONCLUSÕES DA INVESTIGAÇÃO**

O trabalho apresentado revela o modo como uma organização inserida num determinado contexto social e económico vivenciado em Portugal, particularmente árduo nos últimos anos, executou com êxito um plano de continuidade do negócio.

Nesse sentido foi demonstrada a dependência das empresas das TI e os resultados dos períodos de *downtime* através de um estudo realizado a nível global que refere uma perda de receita de 36% e a demora de 34% no desenvolvimento de produtos, para além do que já foi referido, também, aponta para uma taxa baixa, de cerca de 51%, de empresas com *Disaster Recovery*, porém o facto mais alarmante, de cerca de 71%, dos recursos humanos de TI não manterem a confiança na sua aptidão de recuperação da informação.

Foi realizada uma revisão na literatura, no sentido de analisar a execução do PCN na organização, que averiguou as melhores práticas de gestão da continuidade de negócio incluindo a norma ISO 22301.

Posteriormente ao desenvolvimento de uma metodologia de investigação fundamentada no estudo de caso para responder à questão "Como colocar em prática, de modo operacional, um plano de continuidade de negócio?" foi analisado o procedimento de implementação do PCN.

Independentemente da implementação, por parte da organização, de um plano de continuidade de negócio eficiente, a mesma não cumpre com as boas práticas referenciadas na revisão da literatura a 100%.

Para verificar o posicionamento da organização perante a ISO 22301 foi realizada uma apreciação que concluiu que a organização cumpre aproximadamente com 68% das recomendações.

Depois de analisados os resultados foram indicadas medidas para que a organização pudesse alcançar um nível de conformidade aproximado aos 100%.

Após esta investigação é possível concluir que este estudo pretende, acima de tudo, contribuir para as empresas em fase de implementação de um plano de continuidade de negócio oferecendo um conjunto de boas-práticas com o exemplo deste estudo de caso realizado num determinado contexto real específico, bem como com suporte de avaliação do processo perante as boas práticas esclarecidas e perante a norma ISO 22301.

6.2. **LIMITAÇÕES DA INVESTIGAÇÃO**

Esta análise refere-se a uma organização especifica num determinado contexto social e económico em particular. Os resultados que permitiram alcançar as conclusões deste estudo não devem ser generalizados a outros contextos de outras organizações.

6.3. **FUTURAS INVESTIGAÇÕES**

Recomenda-se, para futuras investigações, a realização de estudos similares a empresas do mesmo setor de atividade com a finalidade de obter um suporte de resultados que permita estabelecer a generalização de conclusões a organizações da mesma área de atividade. Recomenda-se, também, que através da investigação se encontrem modelos conceptuais de

avaliação de boas práticas na execução de planos de continuidade de negócio, tanto ao nível de conformidade com a ISO 22301 como na avaliação de um conjunto alargado de boas práticas.

Bibliografia

A Risk Management Standard, 2002, p. 3

Alves, S. (abril de 2009). ANÁLISE Critérios e Parâmetros para Realização do Bia - Business Impact Analysis - no PCN. GESTÃO de RISCOS, p. 48. Obtido em 9 de março de 2017, de Blog da Brasiliano & Associados: www.brasiliano.com.br

ABNT NBR 15999-1 Gestão de Continuidade de Negócios – Parte q – Código de Prática, 2007.

Allocate Software. (julho de 2011). Allocate Software BIA Template July 2011 doc free ebook download from isupport.allocatesoftware.com. Obtido em 23 de fevereiro de 2018, de Ebook Search & Free Ebook Downloads - Ebookbrowse.com: http://ebookbrowse.com/allocate-software-bia-template-july-2011-doc-d226810122

Andrade, D., Vinicius, E., Mafra, G., Flávio, L., Henrique, M., Sepulvedo, U., & Silva, E. (abril de 2011). PLANO DE CONTINGÊNCIA DE TI: PREPARANDO SUA EMPRESA PARA REAGIR A DESASTRES E MANTER A CONTINUIDADE DO NEGÓCIO. FacSENAC/DF, Pós-Graduação em Segurança da Informação da FacSENAC/DF. Distrito Federal - Brasil: Faculdade SENAC.

Australian National Audit Office (ANAO). (2012). checklist Implementation of a business continuity management... Obtido em 23 de fevereiro de 2018, de The Australian National Audit Office: http://www.anao.gov.au/betterpracticeguides/workbook/assets/Checklist%20Undertaking%20a%20business%20impact%20analysis.doc

Balan, M. (22 de janeiro de 2010). Qadit's SecureITy Zone. Obtido em 3 de junho de 2012, de Blog Archive » Managing Risk with ISO 31000: http://www.qadit.com/blog/?p=976

Banco de Portugal. (6 de dezembro de 2010). Relatório da consulta pública do CNSF n.º 1/2010, sobre Recomendações relativas à Gestão da Continuidade de Negócio no sector financeiro. Obtido em 27 de junho de 2017, de Banco de Portugal Eurosistema: http://www.bportugal.pt/ptPT/Supervisao/ConsultasPublicas/Paginas/RelatorioconsultapublicaCNSF1_2010.aspx

Banco de Portugal (BdP), Comissão do Mercado de Valores Mobiliários (CMVM), Instituto de Seguros de Portugal (ISP), no âmbito do Conselho Nacional de Supervisores Financeiros (CNSF), e que se integra no projecto de "Better Regulation" do sector financeiro. Obtido em 13 de agosto de 2017, de Projeto de "Better Regulation": http://www.cmvm.pt/pt/Legislacao/Legislacaonacional/Recomendacoes/Documents/RecCNSFGCN.pdf

BCI, C. (2009). Risk and business continuity management guide. *Business Continuity Institute*.

BCMInstitute, (2014). BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR). Obtido de BCMPedia.org: http://www.bcmpedia.org/wiki/Main_Page

BECKER, H. S. Métodos de pesquisa em ciências sociais. 4. ed. São Paulo: Hucitec, 1999.

Brasiliano, A. C. (março de 2009). Método avançado de análise de risco. Obtido em 19 de agosto de 2017, de Blog da Brasiliano & Associados: http://www.brasiliano.com.br/pdf/metodo_avancado_de_analise_de_riscos.pdf

B&A, Brasiliano & Associados. Gestão de Riscos (Abril 2009, edição 42). Obtido em 19 de agosto de 2017, de Blog da Brasiliano & Associados: file:///C:/Users/antonio/Downloads/edicao_42.pdf

British Standards Institution (BSI). (2010). BCM | Business continuity | BS25999. Obtido em 23 de junho de 2017, de British Standards Institution: http://www.bsigroup.co.uk/en/Assessment-and-Certification-services/Managementsystems/Standards-and-Schemes/BS-25999/

British Standards Institution (BSI). (2011). BS 25999 Continuidade dos Negócios. Obtido em 23 de junho de 2017, de The British Standards: http://www.bsibrasil.com.br/certificacao/sistemas_gestao/normas/bs25999/

British Standards Institution. (31 de outubro de 2011). BS ISO 31100. Obtido em 14 de agosto de 2017, de BS ISO 31100: http://www.talkingbusinesscontinuity.com/bcm-newsand-events/news/bs-311002011-risk-management-code-of-practice-and-guidance-for-theimplementation-of-bs-iso-31000-.aspx

Business Continuity Institute. (janeiro de 2011). Dictionary of Business Continuity Management Terms. Obtido em 13 de junho de 2017, de The Business Continuity Institute: http://www.thebci.org/glossary.htm

Bussines Continuity Institute (BCI). Obtido em 08 de junho de 2017: http://www.thebci.org

California Emergency Management Agency. (6 de junho de 2011). DISCUSSION PAPER Topic: Business Impact Analysis/Assessments. Obtido em 23 de fevereiro de 2017, de Cal E.M.A: http://www.calema.ca.gov/PlanningandPreparedness/Documents/DP BIA 081208.doc

California Emergency Management Agency. (2008). DISCUSSION PAPER Topic: Business Impact Analysis/Assessments. Obtido em 17 de fevereiro de 2017, de Cal E.M.A: http://www.calema.ca.gov/PlanningandPreparedness/Documents/DP BIA 081208.doc

Carvalho, F. d. (Abril de 2009). Expectativa do Mercado para Ferramentas de TI em Gestão de Riscos. Gestão de riscos, pp. 31-34. Obtido em 9 de março de 2017, de Blog da Brasiliano & Associados: www.brasiliano.com.br/blog

Cavalcanti, C. D. (2009). Gestão de Riscos: abordagem de conceitos e aplicações. Obtido em 10 de janeiro de 2017, de http://docplayer.com.br/4505404-Apresentacao-carlos-diego-cavalcanti-dcavalcanti-dcavalcanti-com-gestao-de-riscos-abordagem-de-conceitos-e-aplicacoes.html

Cavalcanti, C. D. (2009). Gestão de Riscos - Abordagem de conceitos e aplicações. Obtido em 10 de abril de 2017, de Convergência Digital Blog publicado por Carlos Diego Cavalcanti Artigos e Análises: http://www.valcann.com/publicacoes/riscos_conceitosaplicacoes.pdf

Centers for Disease Control and Prevention. (30 de junho de 2008). Obtido em 8 de fevereiro de 2017, de Centers for Disease Control and Prevention: http://www2.cdc.gov/cdcup/library/templates/CDC_UP_Business_Impact_Analysis_Template.doc

Cleary, C. (31 de junho de 2005). Measuring Business Results Using Business Impact Analysis - Chief Learning Officer, Solutions for Enterprise Productivity. Obtido em 30 de fevereiro de 2017, de MediaTec Publishing Inc: http://clomedia.com/articles/view/measuring_business_results_using_business_impact_analysis

COBIT. (2013). *Cobit 5 for Assurance.* ISACA. Obtido em 30 de fevereiro de 2017: https://books.google.pt/books?id=FDdbAwAAQBAJ&lpg=PA1&dq=cobit%205&hl=pt-PT&pg=PA2#v=onepage&q=cobit%205&f=false

Computerworld. (Julho de 2010). Computerworld.com.pt. Disaster Recovery, p. 10.

ComputerWorld. (fevereiro de 2011). Computerworld.com.pt. Disaster Recovery, p. 11. Obtido em 2017, de http://www.computerworld.com.pt/.

Computerworld. (julho de 2010). Computerworld.com.pt. Disaster Recovery, p. 10. Obtido em 2017, de http://www.computerworld.com.pt/.

Comunidade ISMS Portugal. (2007). Comunidade Portuguesa de Segurança da Informação. Obtido em 03 de julho de 2017, de Comunidade ISMS PT: Welcome to the ISMS Community Portugal: http://ismspt.blogspot.com/2006/11/pas-56-guia-para-gesto-da-continuidade.html

Continuity SA. (s.d.). Obtido em 23 de fevereiro de 2017, de Business Continuity Management Programs and Disaster Recovery Solutions: http://www.continuitysa.co.za/

Cornish, 2001 Malcom Cornish; The Business Continuity Planning Methodology; The Definitive Handbook of Business Continuity Planning; Wiley; 2001

Disaster Recovery Journal. (2012). Business Continuity Glossary by DRJ. Obtido em 27 de agosto de 2017, de Disaster Recovery Journal: https://www.drj.com/tools/tools/glossary2.html

Estall, H. (6 de outubro de 2010). BSI Shop - Buy British Standards. Obtido em 23 de fevereiro de 2017, de © British Standards Institution 2012: http://shop.bsigroup.com/upload/Standards%20&%20Publications/Risk%20Management/bs25999/HilaryEstall.pdf

Fagundes, E. M. (1996-2012). COBIT. Obtido em 14 de agosto de 2017, de COBIT: http://www.efagundes.com/artigos/cobit.htm

Fagundes, L. L., Karl, F., Baptista, L., & Rosa, R. S. (2010). Estratégias de Contingência para Serviços de Tecnologia da Informação e Comunicação. In U. d. UNISINOS, X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (pp. 249-286). Fortaleza.

Ferrer, R. (s.d.). Continuidad del negócio. Obtido em 23 de Fevereiro de 2017, de SISTESEG COLOMBIA: http://www.sisteseg.com/files/Microsoft_Word__BIA_BUSINESS_IMPACT_ANALYSIS.pdf

Ferrer, R. (s.d.). GESTION DEL RIESGO. Obtido em 10 de setembro de 2017, de SISTESEG COLOMBIA: http://www.sisteseg.com/files/Microsoft_Word__METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

Gallagher, M. (2003). Business Continuity Management - How to Protect your company from danger. Great Britain: Prentice Hall.

George Wrenn, C. (2000-2012). Obtido em 23 de fevereiro de 2017, de Information Security information, news and tips - SearchSecurity.com: http://searchsecurity.techtarget.com/#

Gil, A. C. (2008). Métodos e Técnicas de Pesquisa Social. São Paulo: Editora Atlas, pp. 26-27. Obtido em 23 de fevereiro de 2017: https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf

Gonçalves, H. F. (2011). A gestão do Risco operacional e as TIC - o Contributo da auditoria no setor financeiro. (H. Romão, Ed.) Lisboa: Universidade Católica Editora.

Guindani, A. (2008). Gestão da Continuidade dos Negócios. Obtido em 13 de fevereiro de 2017, de UPIS: http://www.upis.br/posgraduacao/revista_integracao/gestao_continuidade.pdf

Heng, G. M. (26 de julho de 2011). Recovery Time Objective – Recovery Point Objective – Maximum Tolerable Period of Disruption | Business Continuity Planning (BCP) Community. Obtido em 11 de setembro de 2017, de Official Blog for Dr Goh Moh Heng: http://www.gohmoh-heng.com/2011/07/26/bcm-concept-rto-rpo-mtpd/defining-rto/

Heng, (2013). ISO 22301 Documentation Requirements. Consultado em 10 de fevereiro de 2017, de http://www.goh-moh-heng.com/

Heng, (2014). Mapping of BCM Planning Methodology with the ISO 22313 Elements in BC Program. Consultado em 10 de fevereiro de 2017, de http://www.goh-moh-heng.com/

Heng, G. M. (2007). *Managing Sustaining Your Business Continuity Management Program.* GMH.

Hiles, A. (2010). *The definitive handbook of business continuity management.* John Wiley & Sons.

Hiles, A., & Noakes-Fry, K. (2014). *Business Continuity Management: Global Best Practices, 4th Edition.* Rothstein Associates Incorporated. Obtido em 10 de fevereiro de 2017, de https://books.google.pt/books?id=GmX6ngEACAAJ

Human Code. (2010). Relatório de Progresso Estudo de Disaster Recovery. Lisboa.

Infosistema. (2010). Infosistema » Plano Continuidade Negócio. Obtido em 03 de julho de 2017, de Consultoria de TI: http://www.infosistema.pt/consultoria-de-ti/plano-de-continuidade-denegocio/

ISO 27000 Directory. (2008). Introduction To ISO 27005 (ISO27005). Obtido em 14 de agosto de 2012, de Introduction To ISO 27005 (ISO27005): http://www.27000.org/iso27005.htm

ISO 22301. (15 de 05 de 2012). International Standard ISO 22301 Societal security - Business continuity management systems - Requirements. Suiça: ISO.

ISO 22301: 2012 – Societal Segurança – Sistemas de Gestão de Continuidade de Negócio – Requisitos. Consultado em 30 de dezembro de 2017: http://www.bcmpedia.org/wiki/ISO_22301_Glossary (Fonte: ISO 22301).

ISO. ISO/DIS 31.000, Risk management. International Organization for Standardization, 2009. Consultado em 10 de dezembro de 2017: http://www.iso.org/iso/home/standards/iso31000.htm.

ISO22301. (2012). *Business Continuity Management.* British Standards Institution.

Jackson, (2007), a gestão e salvaguarda de Base de Dados vitais, os parâmetros de Segurança, tanto física como lógica, dos sistemas e informação serão revistos durante o processo de implementação do Plano de Continuidade de Negócio.

Kirvan, P. (julho de 2009). Using a business impact analysis (BIA) template: A free BIA template and guide. Obtido em 8 de fevereiro de 2017, de http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-analysis-BIAtemplate-A-free-BIA-template-and-guide

Krause, M., & Tipton, H. F. (s.d.). Handbook of Information Security Management:Risk Management and Business Continuity Planning. Obtido em 23 de junho de 2017, de Handbook of Information Security Management: http://www.blacksheepnetworks.com/security/info/misc/handbook/223-228.html

Mamede, H. S. (2006). Segurança informática nas organizações. Lisboa: FCA - Editora de informática, LDA.

Marciano, J. L. (2006). Segurança da Informação - uma abordagem social. Obtido em 8 de fevereiro de 2012, de VIII ENANCIB "Promovendo a inserção internacional da pesquisa brasileira em Ciência da Informação": www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf

MarkH927@aol.com. (19 de março de 2001). Obtido em 8 de fevereiro de 2017, de AuditNet: Knowledge is Power-Shared Knowledge is AuditNet! The Global Resource for Auditors!: www.auditnet.org/docs/BIA.doc

Martins, J. C., & Belfo, F. (2010). Métodos de investigação qualitativa - Estudos de casos na investigação em sistemas de formação. Proelium n.º 14, 14, 39-71. (T.-C. (. Rouco, Ed.) Lisboa, Lisboa/Lisboa, Portugal/Lisboa: Academia Militar.

Mrasmussen. (24 de novembro de 2009). Good Risk Management Guidance – Here At Last in ISO 31000 Corporate Integrity. Obtido em 03 de junho de 2017, de Corporate Integrity, LLC: http://www.corp-integrity.com/risk-management/good-risk-management-guidance-here-atlast-in-iso-31000

NACIONAL, M. D. (2000). Disaster info desastres. Obtido em 13 de agosto de 2017, de DISASTER info DESASTRES - Partners / PAHO: http://www.disaster-info.net/PEDSudamerica/leyes/leyes/suramerica/brasil/sistemnac/Politica_Nacional_Defensa_Civil.pdf

Nakashima, D. T., & Carvalho, M. M. (3 a 5 de novembro de 2004). XXIV Encontro Nac. de Eng. de Produção. Obtido em 14 de agosto de 2017, de ABEPRO: http://www.abepro.org.br/biblioteca/ENEGEP2004_Enegep0802_1822.pdf

ODE Disaster Recovery Coordinator. (junho de 2008). ODE business impact analysis – June 2008.doc. Obtido em 23 de fevereiro de 2017, de http://www.slideshare.net/: http://www.slideshare.net/Timothy212/ode-business-impact-analysis-june-2008doc

Parreira, A., & Lorga, A. (2013). Transforming ordinal into interval scales. In B. Lausen, S. Krolak-Schwerdt, & M. Böhmer, European Conference on Data Analysis 2013 - Book of Abstracts. Luxembourg: University of Luxembourg.

Pelant, B. F. (19 de julho de 2005). Obtido em 23 de fevereiro de 2017, de Business Resumption Planners Association: http://www.brpa-chicago.org/docs/BRPA%20%20BIA%20Presentation%20(BP).pdf

Pelant, B. F. (19 de julho de 2005). Obtido em 23 de fevereiro de 2017, de Business Resumption Planners Association: http://www.brpa-chicago.org/docs/BRPA%20%20BIA%20Presentation%20(BP).pdf

Pelant, B. F. (19 de julho de 2005). Obtido em 23 de fevereiro de 2017, de Business Resumption Planners Association: http://www.brpa-chicago.org/docs/BRPA%20%20BIA%20Presentation%20(BP).pdf

Portal, T. I. (2008). Introduction to ISO 27005 - ISO27005. Obtido em 3 de junho de 2017, de ISO 27000 Directory 2008 - The ISO 27005 Information Portal (ISO27005 Risk Management): http://www.27000.org/iso-27005.htm

Project Management Institute. (2004). Um guia do conjunto de conhecimentos em gerenciamento de projectos - Guia PMBOK. Four Campus Boulevard, Newtown Square, EUA.

Reis, L. G. (2008). PRODUÇAO DE MONOGRAFIA - DA TEORIA A PRATICA: O METODO EDUCAR PELA PESQUISA (MEP). Brasília: Senac Distrito Federal.

Reto, L., & Nunes, F. (1999). Métodos como estratégia de pesquisa - problemas tipo numa investigação. Revista Portuguesa de Gestão, I, pp. 21-29.

Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002.

Rosa, C. A. (2009). Como elaborar um plano de negócio. Como elaborar um plano de negócio. (S. B. Sebrae, Ed.) Brasilia, Brasilia.

Sanders Glenn, 2002, DMU Business Continuity Plan.

SHARE Inc. (2007). *Business Continuity: The 7-tiers of Disaster Recovery*. [Em linha]. Disponível em: http://recoveryspecialties.com/7-tiers.html [Consultado em 24/09/2017].

SIBS, 2006. Sociedade Interbancária de Serviço "Plano de Continuidade de Negócio" Livro 1 - Visão Global da Continuidade Dezembro 2006, Versão 2.1.2

Silva, P. T., & Torres, C. B. (2010). Gestão e liderança para profissionais de TI. Lisboa: FCA - Editora de Informática.

Sinfic SA. (s.d.). Sinfic SA. Obtido em 29 de junho de 2017, de Sinfic SA: http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=23757

Smith, J. (s.d.). Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP). Obtido em 8 de fevereiro de 2017, de Purdue University: http://www.purdue.edu/securepurdue/docs/training/BusinessContinuityPlanning.ppt

Snedaker, S. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals.* Elsevier Science. Obtido em 8 de fevereiro de 2017: https://books.google.pt/books?id=vT8TAAAAQBAJ

Sonaecom, (2008). Metodologia baseada nas "Good Practice Guidelines", do BCI – Business Continuity Institute (2005/2008). Obtido em 15 de fevereiro de 2017: http://www.sonae.com/CEReports2009/pt/our_governance/risk_management.shtml

Sonaecom. (2009). Sonaecom: Annual Report 2009. Obtido em 03 de junho de 2017, de Sonaecom: Annual Report 2009: http://www.optimus.com.pt/CEReports2009/pt/our_governance/risk_management.shtml

Sousa, M. J., & Baptista, C. s. (2011). Como fazer investigação, dissertações, teses e relatórios segundo Bolonha (3ª ed.). Lisboa: Pactor - Edições de Ciências Sociais e Política Contemporânea.

St-GERMAIN, R. A. (s.d.). ISO 22301 Whitepaper. Social security Business continuity management systems. Proffesional Evalution and Certification Board. Obtido de Professional Evaluation and Certification Board: http://pecb.org/iso22301pt/

Stoneburner, G., Goguen, A., & Feringa, A. (julho de 2002). National Institute of Standards and Technology. Obtido em 3 de outubro de 2017, de NIST.gov - Computer Security Division - Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/80030/sp800-30.pdf

Stoneman, D. (dezembro de 2003). Business Continuity and Business Impact Analysis (BIA) Best Practices. The Issa Journal, p. 4.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002). Contingency Planning Guide for Information Technology Systems. washington: National Institute of Standards and Technology.

Trindade, J. M. (2008). Plano de Continuidade de negócio da sociedade interbancária de serviços (SIBS) - Estudo de Caso numa perspectiva de gestão de beneficios. Lisboa: ISCTE.

Tucker, E. (2014). *Business Continuity from Preparedness to Recovery: A Standards-Based Approach.* Elsevier Science. Retrieved from https://books.google.pt/books?id=v95FBAAAQBAJ

Turnbull, M. (14 de novembro de 2011). Obtido em 23 de fevereiro de 2017, de FORDHAM.EDU: http://www.fordham.edu/images/campus_resources/information_technolo/documents/bia.pdf

UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management. (2002, p.8). A Risk Management Standard.

University of Toronto Information. (2011). CSA - Disaster Recovery Planning. Obtido em 27 de junho de 2017, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#descr

University of Toronto Information. (2012). CSA - Disaster Recovery Planning. Obtido em 10 de fevereiro de 2017, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#descr

Wikipedia. (27 de dezembro de 2011). ISO/IEC 17799/2003. Obtido em 14 de agosto de 2017, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ISO/IEC_17799

Wikipedia. (12 de fevereiro de 2012). Frameworks de melhores práticas ITILv3. Obtido em 14 de agosto de 2017, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ITILv3

WIKIPEDIA. (9 de agosto de 2012). Project Management Body of Knowledge. Obtido em 14 de agosto de 2017, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/Project_Management_Body_of_Knowledge

Wikipedia, t. f. (22 de abril de 2012). ISO 31000 - Wikipedia, the free encyclopedia. Obtido em 3 de junho de 2017, de Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/ISO_31000

Wikipedia, the free encyclopedia. (31 de agosto de 2012). Recovery point objective. Obtido em 11 de setembro de 2017, de Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/Recovery_point_objective

Wikipedia, the free encyclopedia. (23 de junho de 2012). Obsolescência – Wikipédia, a enciclopédia livre. Obtido em 19 de agosto de 2017, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/Obsolesc%C3%AAncia

YIN, R. K. Estudo de caso: planejamento e métodos. 4. ed. Porto Alegre: Bookman, 2010.

Anexos

Recomendações de melhoria com o objetivo de alcançar um nível de conformidade com as boas práticas investigadas, tendo em conta a análise realizada no estudo de caso em causa. As recomendações serão apresentadas por meio de uma tabela por cada ponto analisado, contendo a recomendação, o nível de prioridade (Alta, Media, Baixa) e estimativa de esforço para a concretização da atividade (Baixo, Medio, Elevado).

- **Gestão da Continuidade do Negócio**

Recomendação sobre as boas práticas gerais de gestão da continuidade do negócio encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de Conformidade atual = 86.6%

Tabela 1: Recomendações - Gestão de continuidade do negócio

Recomendação	Prioridade	Esforço
Devem ser implementados controlos e métricas de forma a medir a capacidade global da organização de resposta a incidentes disruptivos.	Média	Elevado
Deve ser feita uma monitorização da performance e efetividade do PCN.	Média	Medio
Os processos de negócio devem sofrer uma reengenharia com vista à melhoria operacional.	Baixa	Elevado

- **Business Impact Analysis (BIA)**

Recomendação sobre as boas práticas gerais de Business Impact Analysis encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de Conformidade atual = 33.3%

Tabela 2: Recomendações – BIA

Recomendação	Prioridade	Esforço
Adicionar a criticidade de recuperação aos processos e sistemas críticos identificados.	Media	Baixo
Rever o BIA e adicionar a informação em falta respeitante aos equipamentos, aplicações e dados necessários após desastre.	Alta	Médio
Adicionar a prioridade de recuperação aos processos e sistemas críticos identificados.	Alta	Baixo

- **Análise Face à ISO 22301**

Recomendações sobre as boas práticas específicas relativas à ISO 22301 encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de Conformidade atual = 68.3.6%

- **Contexto da Organização**

Nível de Conformidade atual = 67.8%

Tabela 3: Recomendações - Contexto da organização

Recomendação	Prioridade	Esforço
Criação de um documento global de risco contendo a estratégia global de risco assim como a apetência ao risco da organização, os fatores que potenciam o risco e definição do critério de risco tendo em conta apetência ao risco.	Alta	Elevado
Criação de um documento com os requisitos legais e regulatórios da sua atividade no que diz respeito à continuidade da atividade. Este documento que deve sofrer atualizações periódicas.	Alta	Elevado
Criação de um documento formal de definição de âmbito do PCN, incluindo natureza, tamanho e complexidade da organização.	Alta	Médio

- **A Liderança e o Papel da Gestão**

Nível de Conformidade atual = 52.3%

Tabela 4: Recomendações – A Liderança e o Papel da Gestão

Recomendação	Prioridade	Esforço
Deverão ser feitas comunicações institucionais periódicas a comunicar reforçar a importância do PCN.	Baixa	Baixo
Deverá ser criado um documento com a política da continuidade da atividade apropriada à atividade pela gestão de topo, contendo critérios de aceitação de risco, uma *framework* de definição de objetivos, enfatizar a melhoria continua, depois de aprovada a politica de continuidade da atividade deverá ser comunicada à organização e revista periodicamente.	Alta	Elevado
Criar um plano de auditoria interna ao PCN.	Alta	Elevado

- **Planeamento**

Nível de Conformidade atual = 68.7%

Tabela 5: Recomendações – Planeamento

Recomendação	Prioridade	Esforço
Criação de um documento formal de objetivos do PCN.	Média	Baixo

- **Suporte do PCN**

Nível de Conformidade atual = 76.7%

Tabela 6: Recomendações – Suporte do PCN

Recomendação	Prioridade	Esforço
Deve ser efetuado uma gestão efetiva de competências do pessoal que executa as operações do PCN, deve existir um documento de gestão de competências do PCN com o registo das diversas competências e deve ser assegurado que o pessoal tem a competência, educação e formação necessárias, sempre que necessário devem ser tomadas ações de forma a fornecer competências ao pessoal, e deve ser mantido um registo de evidencias de competências.	Média	Elevado
Atualização do procedimento de comunicação de modo a incluir a recção, documentação, e resposta a comunicação externa, assim como incluir a comunicação com as autoridades.	Baixa	Baixo
A organização deve tentar adaptar ou integrar um sistema de alerta de ameaças regional ou nacional.	Média	Baixo

- **Operacionalização/Execução**

Nível de Conformidade atual = 83.6%

Tabela 7: Recomendações – Operacionalização/Execução

Recomendação	Prioridade	Esforço
Criar um registo de controlo de execução de processos.	Baixa	Baixo
Alterar o BIA de modo a incluir a definição do critério e contexto da avaliação do impacto disruptivo.	Média	Baixo
Alterar o BIA para incluir uma análise sistemática e priorização de tratamento do risco e custos.	Média	Baixo
Alterar o BIA de modo a especificar os requisitos para que a informação permaneça confidencial.	Média	Baixo
Deverá ser feita uma análise aos potenciais eventos disruptivos e sinalizar os que requerem intervenção.	Média	Médio
Como indicado noutros pontos deverá se atualizado o procedimento de comunicação de modo a garantir a comunicação documentada com as entidades nacionais ou regionais de avisos de risco, onde deverá estar definida a estrutura de comunicação.	Média	Baixo
Devem ser incluídas medidas de bem-estar dos indivíduos no PCN	Baixa	Baixo
Todos os planos devem referenciar as suas interdependências internas e externas, os requisitos de recursos e fluxo de informação.	Média	Baixo
Após a execução do plano de testes devem ser produzidos relatórios com resultados, recomendações e ações de melhoria.	Alta	Médio
Devem ser respeitados os prazos definidos para a realização dos testes e atualização do PCN (anualmente ou sempre que se justifique).	Alta	Elevado

- **Análise da performance**

Nível de Conformidade atual = 54.6%

Tabela 8: Recomendações – Análise da performance

Recomendação	Prioridade	Esforço
Criação de um procedimento de monitorização para monitorizar em que medida o PCN e os seus objetivos são cumpridos, a conformidade dos seus objetivos com o ISO 22301 e que descreva o que deve ser monitorizado e medido, especificar métodos de monitorização, medida, analise e validação que assegurem resultados validos, quando deve ter lugar a monitorização, especificar um conjunto de métricas apropriadas, como resultado do processo devem ser fornecidos indicadores de performance dos processos e procedimentos.	Alta	Médio
Deve ser guardado um histórico com evidências de deficiências auditável.	Baixa	Médio
O resultado do processo de monitorização deve ser guardado de modo a facilitar as ações corretivas.	Médio	Médio
Deve ser estabelecido um plano destinado a estabelecer, implementar e manter um programa de auditorias, incluindo, a frequência, métodos, responsabilidades, requisitos de planeamento e relatório, critérios e âmbito. As auditorias devem ter em conta os resultados de auditorias passadas, o resultado das auditorias devem ser disponibilizados a todos os gestores relevantes para o processo.	Alta	Elevado
Devem ser guardadas evidências auditáveis como prova da implementação do plano de auditoria	Médio	Médio
Sempre que seja encontrada uma não conformidade, deverá ser endereçada.	Alta	Médio
Devem ser guardadas todos os documentos que sejam evidências do tratamento de não conformidades.	Baixa	Baixo
Toda a documentação deve ser guardada, e devem ser tomadas ações apropriadas para implementar as recomendações da auditoria e do plano de monitorização	Alta	Elevado

- **Melhoria**

Nível de Compliance atual = 50%

Tabela 9: Recomendações – Melhoria

Recomendação	Prioridade	Esforço
Deve ser criado um procedimento de identificação e tratamento de não conformidades que deve tentar avaliar a necessidade das ações para eliminar as causas da não conformidade.	Alta	Elevado
As não conformidades devem ser identificadas e aplicadas ações corretivas de modo a eliminar as não conformidades	Alta	Médio
Devem ser guardadas evidências do tratamento de não conformidades.	Baixa	Médio