PAULA SOFIA RICARDO CASQUINHA

GESTÃO DE RISCOS: ANÁLISE DE IMPACTO NO NEGÓCIO

Orientador: Professor Doutor Artur Parreira

Universidade Lusófona de Humanidades e Tecnologias

Escola de Ciências Económicas e das Organizações

Lisboa

2013

PAULA SOFIA RICARDO CASQUINHA

GESTÃO DE RISCOS: ANÁLISE DE IMPACTO NO NEGÓCIO

Dissertação apresentada para a obtenção do Grau de Mestre em Gestão de Empresas, no Curso de Mestrado em Gestão de Empresas, conferido pela Universidade Lusófona de Humanidades e Tecnologias.

Orientador: Professor Doutor Artur Parreira

Universidade Lusófona de Humanidades e Tecnologias

Escola de Ciências Económicas e das Organizações

Lisboa

2013

"O que diferencia um risco de uma incerteza é o conhecimento."
(MENEZES, 2009)

Dedico este trabalho à minha filha, ao meu companheiro, aos meus pais e irmão que me inspiraram e fizeram sempre querer continuar e melhorar.
Ao orientador, pela sabedoria na orientação e amizade dispensada.

RESUMO

O objetivo deste estudo é identificar dentro de um instituto público, um cenário tecnológico para recuperação de negócio através de soluções de recuperação de baixo investimento e que permita simultaneamente a redução das despesas operacionais.

Para a elaboração do presente estudo foi utilizada a metodologia de investigação científica de estudo de caso com propósito exploratório de forma a obtenção de respostas às questões propostas.

Relativamente ao estado da arte adotou-se uma metodologia baseada na investigação da literatura referente ao plano de continuidade de negócio, gestão de risco, análise de risco e avaliação ou análise de impacto de negócio.

Da pesquisa efetuada, através de consultadoria externa, concluiu-se que, por aplicação da metodologia Análise do impacto nos negócios, os sistemas considerados extremamente críticos e estratégicos para a organização são o sistema de correio eletrónico, sistema central de diretório, repositório de ficheiros e o principal sistema de informação de suporte ao negócio.

Foi ainda possível identificar, através do estudo de caso os cenários de recuperação de desastres que melhor se ajustam à situação atual da organização em estudo, por responderem às questões da pesquisa.

Palavras-chave: gestão de riscos, análise de impacto de negócio, continuidade de negócio, recuperação de desastres.

ABSTRACT

The aim of this study is to identify within a public Institute, a technological scenario for business recovery via recovery solutions of low investment and enabling the simultaneous reduction in operating expenses.

For the preparation of the present study was used the methodology of scientific research of case study with exploratory purpose in order to obtain answers to the questions proposed.

Regarding the State of the art adopted a methodology based on the research literature concerning the business continuity plan, risk management, risk analysis and assessment or business impact analysis.

The research carried out by external consultants, it was concluded that, by application of the business impact analysis methodology, systems considered extremely critical and strategic for your organization are the email system, central system directory, file repository and the main information system of business support.

It was even possible to identify, through the case study disaster recovery scenarios that best fit the Organization's current situation in study, respond to issues of research.

Key words: risk management, business impact analysis, business continuity, disaster recovery.

ABREVIATURAS, SIGLAS E SÍMBOLOS

AIRMIC	*The Association of Insurance and Risk Managers*
ALARM	*The National Forum for Risk Management in the Public Sector*
AR	Alto Risco
BCI	*The Business Continuity Institute*
BCM	Gestão de continuidade de negócio ou acrónimo do inglês *«Business continuity management»*
BCP	Plano de continuidade de negócio ou acrónimo do inglês *«Business continuity planning»*
BIA	Análise do impacto nos negócios ou acrónimo do inglês «*Business Analysis Impact*»
BSI	*British Standards Institution*
CAPEX	Despesas de capital ou investimento em bens de capital ou acrónimo do inglês «*capital expenditure*»
CD	Conselho Diretivo
CDP	Proteção de dados contínua ou acrónimo do inglês *«Continuous Data Protection»*
CPU	Unidade central de processamento ou acrónimo do inglês «*Central Processing Unit*»
DHCP	Protocolo de configuração dinâmica de anfitrião ou acrónimo do inglês *« Dynamic Host Configuration Protocol»*
DNS	Serviço de resolução de nomes ou acrónimo do inglês *«Domain Name System»*
E-business	Negócio eletrônico ou acrónimo do inglês «*Electronic Business*»
GB	*«Gigabyte»*
IRM	*UK – The Institute of Risk Management*
ISO	Organização Internacional de Normalização
LDAP	Sistema central de diretório ou acrónimo do inglês «*Lightweight Directory Access Protocol*»
MAR	Modelo de avaliação de risco
MTD	Tempo máximo tolerável de inatividade ou acrónimo do inglês «*Maximum Tolerable Downtime*»
NLB	Balanceador de carga
OPEX	Despesas operacionais ou acrónimo do inglês «*operational expenditure*»
PCN	Plano de continuidade de negócio
PMBOK	*Project Management Body of Knowledge*
PMI	*Project Management Institute*
PRD	Plano de recuperação de desastres
RAM	Memória de acesso aleatório ou acrónimo do inglês «*Random Access Memory*»
RB	Baixo Risco

RE	Risco Elevado
RM	Risco Médio
RPO	Objetivo de ponto de recuperação ou acrónimo do inglês «R*ecovery point objective*»
RTO	Objetivo de tempo de recuperação ou acrónimo do inglês «*Recovery time objective*»
SDLC	Ciclo de vida de desenvolvimento de sistema ou acrónimo do inglês «*System Development Life Cycle*»
SI	Sistemas de informação
SRM	Gestão de Recursos de Armazenamento ou acrónimo do inglês «*Storage Resource Management*»
TCO	Custo total da posse ou acrónimo do inglês «*Total cost of ownership*»
TI	Tecnologias de Informação
WAN	Rede de área alargada ou Rede de longa distância ou acrónimo do inglês «*Wide Area Network*»
WWW	Teia mundial ou acrónimo do inglês World Wide Web

ÍNDICE

1 Introdução 14

1.1 Problema 14

1.2 Formulação de situação 15

1.3 Objetivos 15

1.3.1 Objetivo Geral 15

1.3.2 Objetivos Específicos 16

1.4 Delimitação do estudo 16

1.5 Justificação e relevância do estudo 16

1.6 Questões da pesquisa 17

1.7 Organização do estudo 17

2 Fundamentação teórica 19

2.1 Plano de continuidade de negócio 19

2.1.1 Definições e Conceitos 20

2.1.2 Evolução histórica 24

2.1.3 10 Elementos fundamentais 25

2.1.4 Metodologia para elaborar um plano de continuidade de negócio 25

2.1.5 Fases do projeto de Continuidade de Negócio 27

2.1.6 Benefícios esperados da Continuidade de Negócio 33

2.2 Gestão de risco 34

2.2.1 Benefícios da gestão de risco 37

2.2.2 Dicionário de riscos 37

2.2.3 Metodologia 38

2.3 Análise Risco 46

2.3.1 Metodologia da Análise de Risco 49

2.3.2 Principais Normas 51

2.4 Análise ou avaliação de impacto de negócio 52

2.4.1 Elementos chave da análise BIA 56

2.4.2 Metodologia 57

2.4.3 Objetivos....60
2.4.4 Benefícios....61
2.4.5 Exemplos de atividades críticas....61

3 Metodologia de pesquisa....62

3.1 Estratégia de pesquisa....62
3.1.1 Pesquisa exploratória....62
3.1.2 Estudo de caso....63

3.2 Instrumentos de pesquisa....65
3.2.1 Aplicação dos instrumentos....65

3.3 Análise dos dados....65

4 Estudo de caso....66

4.1 Caracterização do Instituto Público....66

4.2 Caracterização do negócio....66

4.3 Gestão do negócio....67
4.3.1 Situação atual....67

4.4 Valoração económica....70

4.5 Projeto de Recuperação de desastres....71

4.6 Cenários....72
4.6.1 Projeções económicas....73
4.6.2 Mapa comparativo de cenários....73

5 Análise e interpretação de dados e Recomendações derivadas do modelo....74

6 Perspetivas de trabalho futuro....76

Bibliografia....77

Obras Citadas....84

Glossário....87

Índices Remissivos....94

Anexos.....XCVI

ÍNDICE DE TABELAS

Tabela 1 - Modelo Genérico de matriz de exposição a riscos (probabilidade versus impacto)21
Tabela 2 - Seleção de critérios de site alternativo 32
Tabela 3 - Medição das consequências face às ameaças 35
Tabela 4 - Metodologia de processo de avaliação de risco 40
Tabela 5 - Probabilidade de ocorrência de ameaças 42
Tabela 6 - Lista de critérios de segurança para identificação de vulnerabilidades 43
Tabela 7 - Classificação geral de probabilidade 44
Tabela 8 - Tabela resumo das categorias de impacto no negócio 45
Tabela 9 - Fontes típicas de risco, por categoria 48
Tabela 10 - Descrição dos riscos 50
Tabela 11 - Relação do nível de tolerância/tempo 55
Tabela 12 - Metodologia de análise BIA 57
Tabela 13 - Características principais do método estudo de caso 64
Tabela 14 - "As Is" no âmbito das tecnologias/sistemas de informação e comunicação 68
Tabela 15 - Listagem de servidores 69
Tabela 16 - Elementos para valoração económica 70
Tabela 17 - Projeções económicas para as soluções em euros 73
Tabela 18 - Mapa comparativo de cenários de recuperação de desastres 73

ÍNDICE DE FIGURAS

Figura 1- Definindo RPO, RTO e MTD 23
Figura 2 -Evolução da continuidade do negócio 24
Figura 3 - Elaboração do plano de projeto para implementação das medidas 25
Figura 4 - Abordagem à Gestão de Continuidade de Negócio 27
Figura 5 - Atividades Principais do Plano 28
Figura 6 - Principais fases do BCM 29
Figura 7 - Ciclo de Gestão de Risco 29
Figura 8 - Análise de risco dos processos de SI/TI 30
Figura 9 - Fase de implementação 32
Figura 10 - Fases de Recuperação definidas pelo Plano de Continuidade Negócio 33
Figura 11 - Cadeia de valor de riscos e processos, considerando as condições externas e internas 38
Figura 13 – Exemplo Matriz Impacto x Magnitude - Análise de Riscos 50
Figura 14 - Matriz de Risco 51
Figura 15 - Exemplo de um ficheiro com análise BIA 54
Figura 16 - Elementos chave da análise BIA 56
Figura 17 - Perspetiva do Estudo no contexto do Projeto Global de «Disaster Recovery» 72

1 INTRODUÇÃO

1.1 PROBLEMA

O acesso ininterrupto e constante aos sistemas de informação e à própria informação são fundamentais em qualquer organização, pelo que a disponibilidade, segurança, fiabilidade e o acesso atempado à informação são fatores essenciais para o normal funcionamento de uma organização.

Com o aumento da dimensão do negócio e o aparecimento de questões relacionadas com risco de indisponibilidade dos negócios, isto é, probabilidade de ocorrer descontinuidade de negócio provocada por interrupções causadas, por exemplo, por incêndios, sabotagem, pandemia, acidentes aéreos, entre outros, impõe a implementação de novas regras, procedimentos de validação de forma a proteger a informação e os sistemas de informação. Assim, é fundamental para um gestor de Tecnologias de Informação/Sistemas de Informação sensibilizar os administradores das organizações para a implementação de um plano de continuidade de negócio e plano de recuperação de desastre.

Um Plano de Continuidade de Negócio[1] tem diversos componentes: análise de riscos; análise de impacto de negócio, planos de contingência/estratégia e validação de testes/procedimentos[2]. Das componentes ou etapas referidas anteriormente a análise de impacto de negócio ou *«Business Analysis Impact»*[3] e definição de planos de estratégia tecnológica serão o objeto do presente trabalho de dissertação. Através destas componentes será possível definir a melhor estratégia para um plano de recuperação de desastres.

A análise BIA permite ao gestor ter uma visão estratégica de continuidade de negócio, permitindo que este priorize os processos de negócio mais relevantes na organização, a dois níveis: impacto no negócio e nível de tolerância. Só assim será possível proceder ao desenvolvimento dos planos de contingência/recuperação.

As decisões baseadas no Impacto no Negócio apoiam a organização na tomada de determinados tipos de decisões que os indicadores não suportam, pois o impacto no negócio é uma medida financeira. Reconhecer o real impacto das atividades das Tecnologias de Informação «TI»/Sistemas de Informação «SI» para a organização é fator crítico de sucesso para a determinação de projetos, ações e decisões empresariais, visando a saúde organizacional e a sua continuidade (Carvalho, 2009).

[1] PCN
[2] Rever periodicamente todos os testes e procedimentos criados durante as diversas fases do PNC
[3] BIA

1.2 FORMULAÇÃO DE SITUAÇÃO

O caso de estudo tem como objeto um Instituto Público cuja missão está focada na gestão integrada das políticas ambientais, de forma articulada com outras políticas setoriais, tendo em vista um elevado nível de proteção e de valorização do ambiente.

Este Instituto Público tem realizado altos investimentos em TI/SI, na medida em que procedeu à informatização da totalidade do seu negócio, controlando de forma mais eficiente os diversos processos de licenciamento pelos quais é responsável.

Estando os dirigentes do Instituto Público conscientes das perdas que advêm dos riscos a que os SI/TI estão potencialmente expostos, propôs-se ao Conselho Diretivo[4] identificar os processos de negócio extremamente críticos e estratégicos para a organização, através da metodologia BIA e optar por um cenário tecnológico para recuperação de negócio através de soluções de «*Disaster Recovery*», de baixo «*Capex*», que permita simultaneamente a redução do «*Opex*».

O presente estudo faz parte de um estudo mais abrangente para a realização de um PCN para todo o Instituto Público, fazendo assim parte da integrante da estratégia definida pelo CD.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

O objetivo deste estudo é identificar os processos de negócio extremamente críticos e estratégicos para a organização, através da metodologia BIA e optar por um cenário tecnológico para recuperação de negócio através de soluções de «*Disaster Recovery*», de baixo «*Capex*», que permita simultaneamente a redução do «*Opex*».

É essencial ter conhecimento dos processos de negócio críticos dentro da organização.

[4] CD

Só assim é possível responder às seguintes questões: Quais os processos de negócio extremamente críticos e estratégicos para a organização? Qual a solução tecnológica com menor custo e que se ajusta aos parâmetros definidos nos objetivos específicos?

1.3.2 OBJETIVOS ESPECÍFICOS

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

- Mirror Site[5]: RTO < 1h e RPO = 0 horas
- Backup[6] Site: RTO < 8h e RPO < 24 horas

1.4 DELIMITAÇÃO DO ESTUDO

A identificação das aplicações críticas revelou-se um trabalho complicado considerando que não foi possível aplicar o questionário de análise de impacto de negócio em anexo (Anexo 1).

De forma a dar resposta à primeira questão "Quais os processos de negócio extremamente críticos e estratégicos para a organização?" foi necessário recorrer ao estudo realizado através de consultadoria externa, cujos resultados foram aferidos com base na metodologia BIA.

A limitação identificada reduz a abrangência desta dissertação e conduz a que a presente análise académica não seja tão abrangente como desejável para ser utilizável por entidades com o mesmo negócio.

O nome da entidade e dos técnicos que apoiaram no levantamento dos riscos foram omissos, com a finalidade de preservar as fontes.

1.5 JUSTIFICAÇÃO E RELEVÂNCIA DO ESTUDO

A principal razão da escolha do tema resulta da sua atualidade, uma vez que o Gestor de Topo necessita de saber o risco a que o seu Instituto está exposto e o nível de risco que está disposto a aceitar, definindo assim o nível de controlo que pretende garantir de forma a assegurar a recuperação de desastres e continuação do negócio.

[5]Espelho ou acrónimo do inglês «*mirror*» significa cópia exata de um «*site*»
[6]É a cópia de dados de um dispositivo de armazenamento a outro (CD-ROM, DVD, disco rígido, disco rígido externo (compatíveis com USB), fitas magnéticas e a cópia de segurança externa (online) para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver desaparecimentos acidentais ou corrupção de dados.

A disponibilidade, segurança, fiabilidade e acesso atempado e ininterrupto à informação são fatores essenciais para o normal funcionamento de uma organização, impondo-se a implementação de regras, procedimentos, auditorias e processos de validação que permitam proteger a informação e os sistemas de informação.

De forma a ser possível ao gestor ter uma visão global da sua organização e poder aferir os riscos a que a organização está sujeita é fundamental que se proceda à elaboração de uma análise de impacto de negócio. Esta análise permitirá ao gestor ter uma visão estratégica de continuidade de negócio, na medida em que permite priorizar os processos de negócio, em conformidade com o respetivo impacto e o nível de tolerância e, ao decisor tomar decisões sobre o nível de controlo que pretende garantir face aos riscos a que o Instituto está exposto e consequentemente o nível de risco que está disposto a aceitar.

1.6 QUESTÕES DA PESQUISA

Quais os processos de negócio extremamente críticos e estratégicos para o Instituto?

Qual a solução tecnológica com menor custo e que se ajusta aos parâmetros definidos nos objetivos específicos?

1.7 ORGANIZAÇÃO DO ESTUDO

A dissertação encontra-se estruturada por 6 capítulos e subcapítulos, por forma a possibilitar uma melhor entendimento da mesma.

No capítulo 1 encontra-se a introdução deste estudo, onde se salienta a importância da utilização de um modelo de impacto de negócio como forma de estimar e minimizar as interrupções em atividades críticas, considerando o tempo de recuperação dessas atividades. Este capítulo inclui também a formulação do problema, os objetivos gerais e específicos, as delimitações do estudo, assim como a justificação e relevância para a elaboração do mesmo. Encontram-se ainda as questões a que o estudo pretende dar resposta e a presente organização do trabalho.

No capítulo 2 encontra-se a fundamentação teórica do estudo, que se encontra dividida em quatro ramos: plano de continuidade de negócios, gestão de risco, análise de risco e análise de impacto de negócio.

O capítulo 3 refere a metodologia de pesquisa adotada para a elaboração deste estudo.

O capítulo 4 apresenta o estudo de caso, onde é feita a descrição da entidade estudada bem como a análise de impacto de negócio realizada. Neste capítulo também são apresentados

os vários cenários de recuperação de desastre que se melhor se adaptem aos parâmetros definidos no Capítulo 1.

No capítulo 5 são apresentadas as considerações sobre as questões colocadas na investigação, onde se contempla as conclusões retiradas ao longo da dissertação, através da investigação e das várias análises efetuadas seguindo-se as perspetivas do trabalho futuro.

Nos Anexos encontram-se o formulário proposto para análise de impacto de negócio, reflexões do pré-teste do questionário, os cenários de estratégia de recuperação de negócio realizada no estudo de caso e as recomendações para o projeto-piloto tecnológico de recuperação de desastres.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 PLANO DE CONTINUIDADE DE NEGÓCIO[7]

O despertar para planos de recuperação de desastres e continuidade de negócio iniciou-se em 2001, com o atentado terrorista do 11 de Setembro às Torres Gémeas.

Atualmente, em Portugal, parece haver uma maior consciencialização para a necessidade de as organizações se precaverem dos riscos de perdas de dados de negócio.

Normalmente, o primeiro passo para preparar o plano de continuidade do negócio é organizar os responsáveis internos da organização e obter o apoio dos órgãos de decisão para o conceito, considerando que estes reconhecem o seu valor, mas ainda não o assumem como essencial.

A disponibilização de soluções de recuperação de sistemas e informação crítica para a organização, a existirem, devem ser flexíveis e economicamente viáveis.

As organizações precisam de ser capazes de recuperar rapidamente de um desastre natural ou de uma falha de serviço, de forma a minimizarem as suas perdas.

Segundo Gallagher (2003), existem 3 elementos chave que se devem considerar quando se aborda o tema de continuidade de negócio:

- Antecipar incidentes;
- Saber que funções afetar e a que processos críticos;
- Assegurar que a resposta a qualquer incidente é devidamente planeada e testada.

O Plano de continuidade de negócio deverá existir e deverá incluir um Plano de Recuperação de Desastres[8].

Um plano de continuidade de negócio é composto por:

- Plano de resposta de emergência - Informação necessária para salvar pessoas e bens numa primeira fase;
- Plano de gestão de crise - Controlado pela equipa de crise criada para o efeito e que regula todo o comportamento da organização durante o período de crise;
- Plano de recuperação tecnológica para os sistemas de TI de suporte ao negócio;
- Plano de processos alternativos de negócio, que permite à organização continuar as suas operações mínimas durante o período de crise.

[7] PCN
[8] PRD

2.1.1 DEFINIÇÕES E CONCEITOS

O Business Continuity Institute (BCI) define o PCN como um ato de antecipar incidentes que afetarão as funções de missão e processos críticos para a organização, garantindo que o plano responde a qualquer incidente, de forma planeada e ensaiada (Business Continuity Institute, 2011).

Para a Infosistema (Infosistema, 2010) o PCN é um processo de Gestão cujo objetivo é manter e repor os processos de negócio, após uma disrupção grave dos mesmos, incluindo a gestão de todos os recursos necessários para produção, nomeadamente pessoas e bens.

De forma geral, pode-se definir o PCN com um plano para a resposta à emergência, operações «*backup*» e recuperação de ativos atingidos por uma falha ou desastre de forma a assegurar a disponibilidade de recursos de sistema críticos, recuperar um ambiente avariado e promover o retorno à sua normalidade.

2.1.1.1 Segurança e Risco

Os dois conceitos estão diretamente interligados com a continuidade de negócio e de certa forma ambos precedem a implementação de um plano desta natureza.

Relativamente ao risco é necessário realizar uma análise de riscos (capítulo 2.3) antes de se elaborar uma estratégia de continuidade.

2.1.1.2 Impacto versus probabilidade

A construção de uma matriz desta natureza permite definir prioridades para as ações corretivas que se fizerem necessárias em cada um dos sistemas e nos processos críticos de negócio.

Tabela 1 - Modelo Genérico de matriz de exposição a riscos (probabilidade versus impacto) [9]

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)

A escala utilizada na Tabela 1 - Modelo Genérico de matriz de exposição a riscos (probabilidade versus impacto) , foi a apresentada na Conferência Europeia de Análise de Dados por Parreira & Lorga (2013)[10].

Trata-se de uma escala de intervalos com base no valor numérico atribuído pelas pessoas aos advérbios de quantidade.

O valor numérico dos advérbios utilizados na escala da tabela 1 foram os seguintes:

- Extremamente com o valor numérico de 9,25;
- Bastante com o valor numérico de 7,08;
- Medianamente com o valor numérico de 4,62;
- Pouco com o valor numérico de 2,27;
- Nada com o valor numérico de 0,54.

[9] Adaptado de Cavalcanti, 2009, p. 25
[10] Parreira & Lorga, Transforming ordinal into interval scales, 2013

2.1.1.3 Prejuízo versus Impacto

Os prejuízos são o custo de perda de infraestrutura.

O impacto refere-se às consequências, pelo facto da organização se encontrar impossibilitada de dar continuidade ao seu negócio. Os impactos podem ser de curto, médio e longo prazo. Os impactos podem ser diretos quando traduzem a perda da infraestrutura onde assentava o negócio e a perda de informação e indiretos quando se verifica a impossibilidade de se executar algumas funções da organização.

A análise de impacto deve quantificar os efeitos da probabilidade de ocorrência de um desastre.

2.1.1.4 Objetivo de ponto de recuperação/*Recovery point objective (RPO)*

Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização.

O RPO permite que a organização defina uma janela de tempo, antes de um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais. Esta métrica pode ser expressa em volume de dados ou pelo tempo que decorre entre as atualizações de dados. O que diferencia o tempo de RPO é a tecnologia que a organização utiliza para fazer a atualização dos dados.

De forma mais simples RPO significa tempo máximo durante os quais os dados não foram salvaguardados, antes do desastre (tempo para trás).

Por exemplo, um RPO de 24 horas significa que a janela máxima de dados perdidos é 24 horas.

2.1.1.5 Objetivo de tempo de recuperação/*Recovery time objective* (RTO)

Período a partir do qual todos os dados e serviços críticos têm de estar operacionais. Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a organização entende por "perda aceitável" numa situação de desastre.

O RTO permite que a organização defina uma janela de tempo, antes de um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais.

Assim sendo, RTO é o período de tempo necessário para recuperar os sistemas ou aplicações, ou seja, representa o período de tempo que medeia entre a anomalia e a recuperação de uma determinada função de negócio através da ativação da resposta prevista no PCN, definido geralmente pelo grau de criticidade das funções.

De forma mais simples, RTO é o tempo máximo para trazer os sistemas de novo «*Online*», após desastre ou interrupção dos serviços.

Por exemplo, um RTO de 4 horas significa que o sistema deve estar recuperado 4 horas após um desastre ou interrupção dos serviços.

2.1.1.6 Tempo máximo tolerável de inatividade/*Maximum Tolerable Downtime* (MTD)

Especifica o período máximo de tempo que um determinado processo empresarial pode estar inoperante antes de a sobrevivência da organização estar em risco.

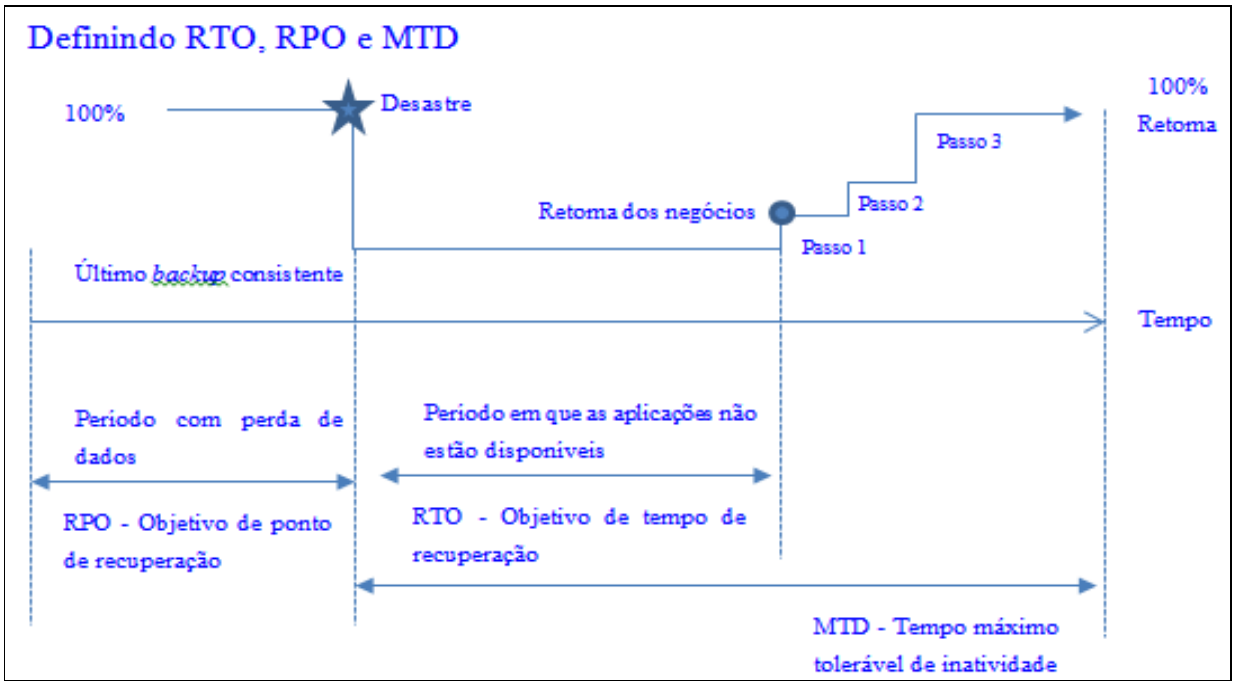


Figura 1- Definindo RPO, RTO e MTD

(Adaptado de Heng, 2011)

2.1.2 EVOLUÇÃO HISTÓRICA

Com a Era do Computador teve inicio a preocupação das organizações e dos responsáveis pelos sistemas computacionais, com a segurança e com mecanismos que, de alguma forma, garantissem a continuidade do negócio (Guindani, 2008).

A evolução do processo de continuidade de negócios é contínua, mantendo um planeamento das atividades e recursos sempre atualizados em conformidade com a evolução do negócio da organização.

O histórico da evolução do conceito de continuidade do negócio é apresentado na figura seguinte:

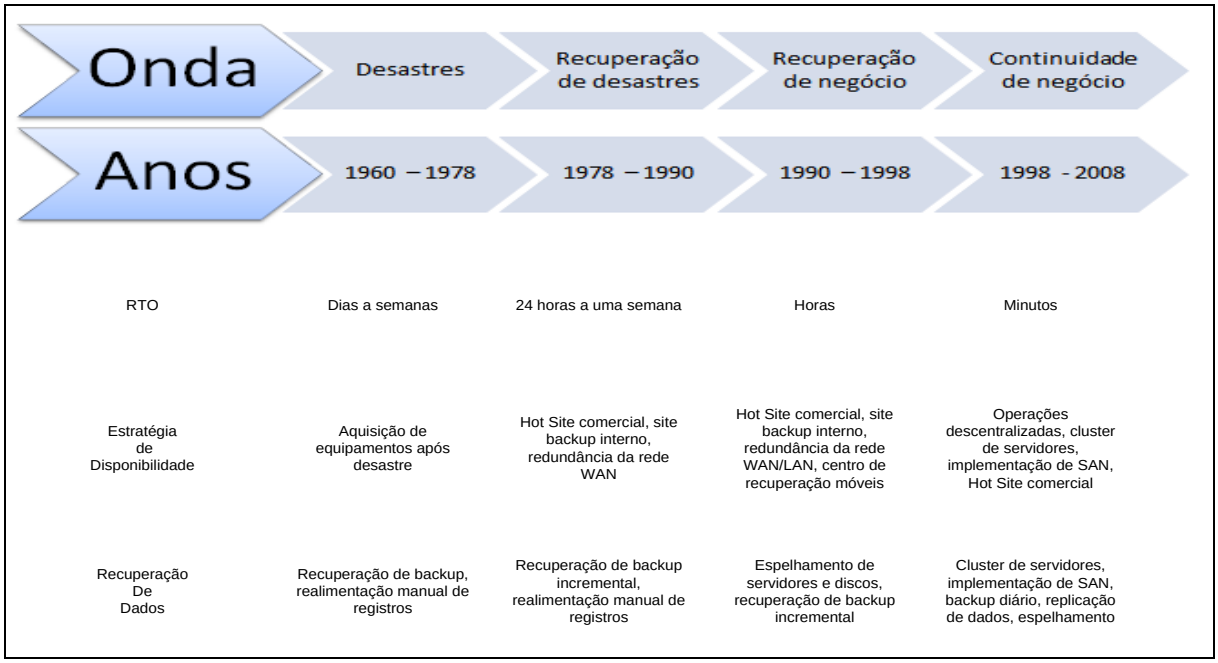


Figura 2 -Evolução da continuidade do negócio[11]

A partir de 1980 a oferta de serviços na área de recuperação de «*sites*» aumenta, dando origem a centros de recuperação sofisticados.

A partir de 1990 o foco passa do PRD para o BCP que passa para o «*Business continuity Management*» (BCM).

Ocorreram inúmeros acontecimentos e fatores que foram considerados como impulsionadores da continuidade do negócio, tais como:

- «*Bug*» do milénio;
- O 11 de setembro de 2001.

[11] Adaptado de Guindani, 2008

É em 2001 que os Órgãos de gestão começam a aperceber-se que a sobrevivência das organizações pode vir a depender da implementação da BCM.

2.1.3 10 ELEMENTOS FUNDAMENTAIS

Quando se arquiteta um plano desta natureza é necessário considerar 10 elementos fundamentais, tal como é referido na revista *Computerworld*, de Julho de 2010[12]. Os elementos a considerar são:

- Definir quem são os responsáveis e obter apoio dos órgãos de decisão;
- Justificar o plano;
- Definir bem o plano;
- Identificar os erros mais importantes;
- Estabelecer relações com as lições da vida real;
- Entender o negócio;
- Identificar custos de indisponibilidade;
- Retirar os dados das instalações;
- Pensar além do suporte de *backup*;
- Melhorar a continuidade de negócio com a virtualização ou com uma solução de alojamento em nuvem.

2.1.4 METODOLOGIA PARA ELABORAR UM PLANO DE CONTINUIDADE DE NEGÓCIO

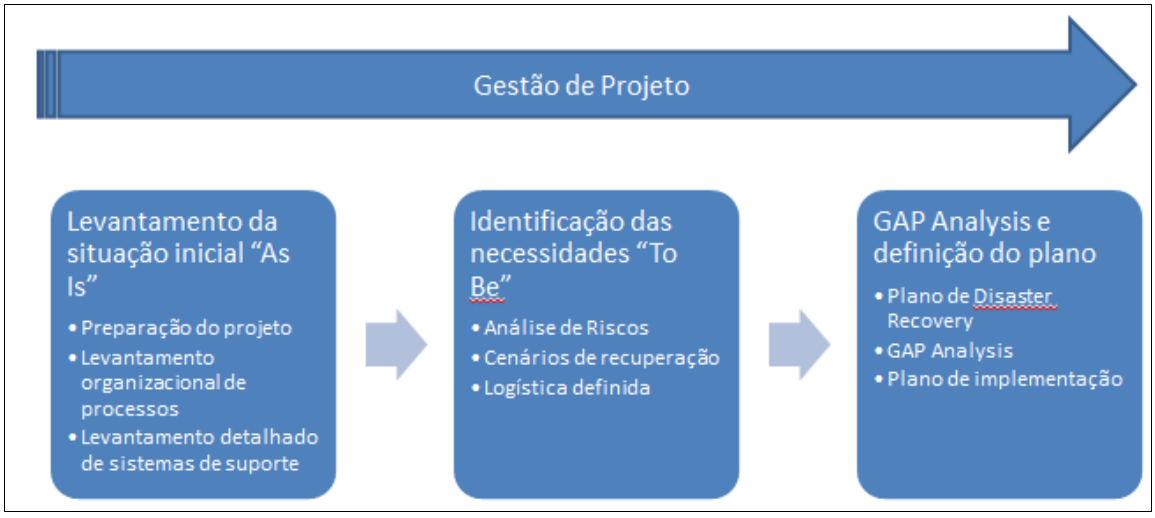


Figura 3 - Elaboração do plano de projeto para implementação das medidas[13]

[12] *Computerworld*. (Julho de 2010). Computerworld.com.pt. *Disaster Recovery*
[13] Adaptado de Infosistema, 2010

Por outro lado e, segundo a University of Toronto Information (University of Toronto Information, 2011)[14], deve-se considerar os seguintes pontos-chave:

- Os órgãos de gestão terem uma compreensão abrangente do esforço total necessário para desenvolver e manter um plano de recuperação eficaz;
- Obter o compromisso dos órgãos de gestão adequada para apoiar e participar no esforço;
- Definir de requisitos de recuperação a partir da perspetiva de funções de negócios;
- Documentar o impacto de uma perda estendido para operações e funções chave de negócio;
- Manter o foco adequado sobre prevenção de desastres e minimização de impacto, bem como a recuperação ordenada;
- Selecionar equipa de projeto que garanta o equilíbrio necessário para o desenvolvimento do plano;
- Desenvolver um plano de contingência que seja compreensível, fácil de usar e fácil de manter;
- Serem integrados no planeamento os negócios em curso e processos de desenvolvimento de sistema.

[14] University of Toronto Information. (2011). CSA - Disaster Recovery Planning. Obtido em 27 de Junho de 2011, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#descr

2.1.5 FASES DO PROJETO DE CONTINUIDADE DE NEGÓCIO[15]

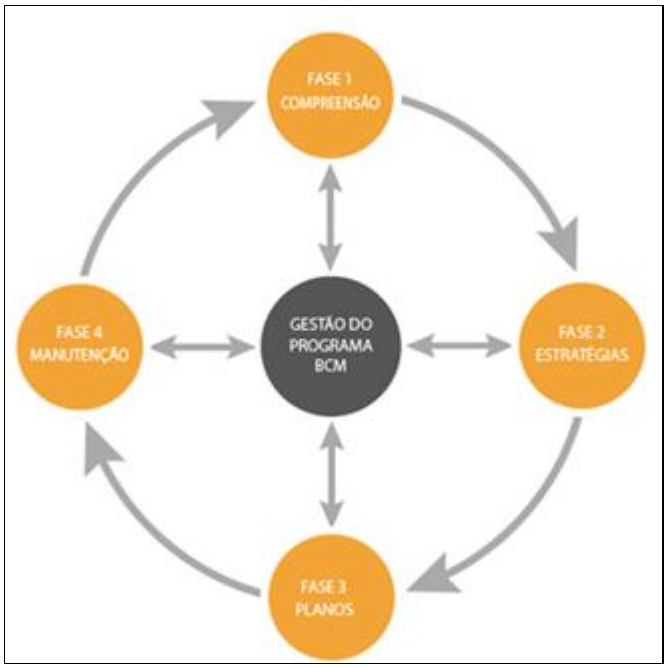


Figura 4 - Abordagem à Gestão de Continuidade de Negócio[16]

De seguida descreve-se cada fase de forma sucinta:

- Fase 1 refere-se à compreensão do negócio, isto é, compreende a elaboração da análise de impacto de negócio, a avaliação dos riscos e definição da abrangência do BCM;
- Fase 2 integra a definição de estratégias de BCM, incluindo as seguintes tarefas: identificação e caraterização de estratégias de recuperação, definição de medidas para gerir os riscos, análise de vantagens e desvantagens por cada estratégia definida;
- Fase 3 concerne ao desenvolvimento implementação de planos BCM, que engloba: planos de gestão de crise, planos de continuidade de negócio, desenvolvimento e implementação de soluções de continuidade;
- Fase 4 refere-se à manutenção, testes e auditoria do BCM e engloba as seguintes tarefas: manutenção dos planos de continuidade, teste e simulações aos planos, auditoria aos processos BCM.

[15] BCM
[16] Adaptado de Sonaecom, 2009

Para que um projeto desta natureza seja conveniente implementado é necessário "…embeber a cultura BCM na organização…" (Sonaecom, 2009) através de divulgação e formação aos técnicos, monitorização da mudança e implementação da cultura BCM.

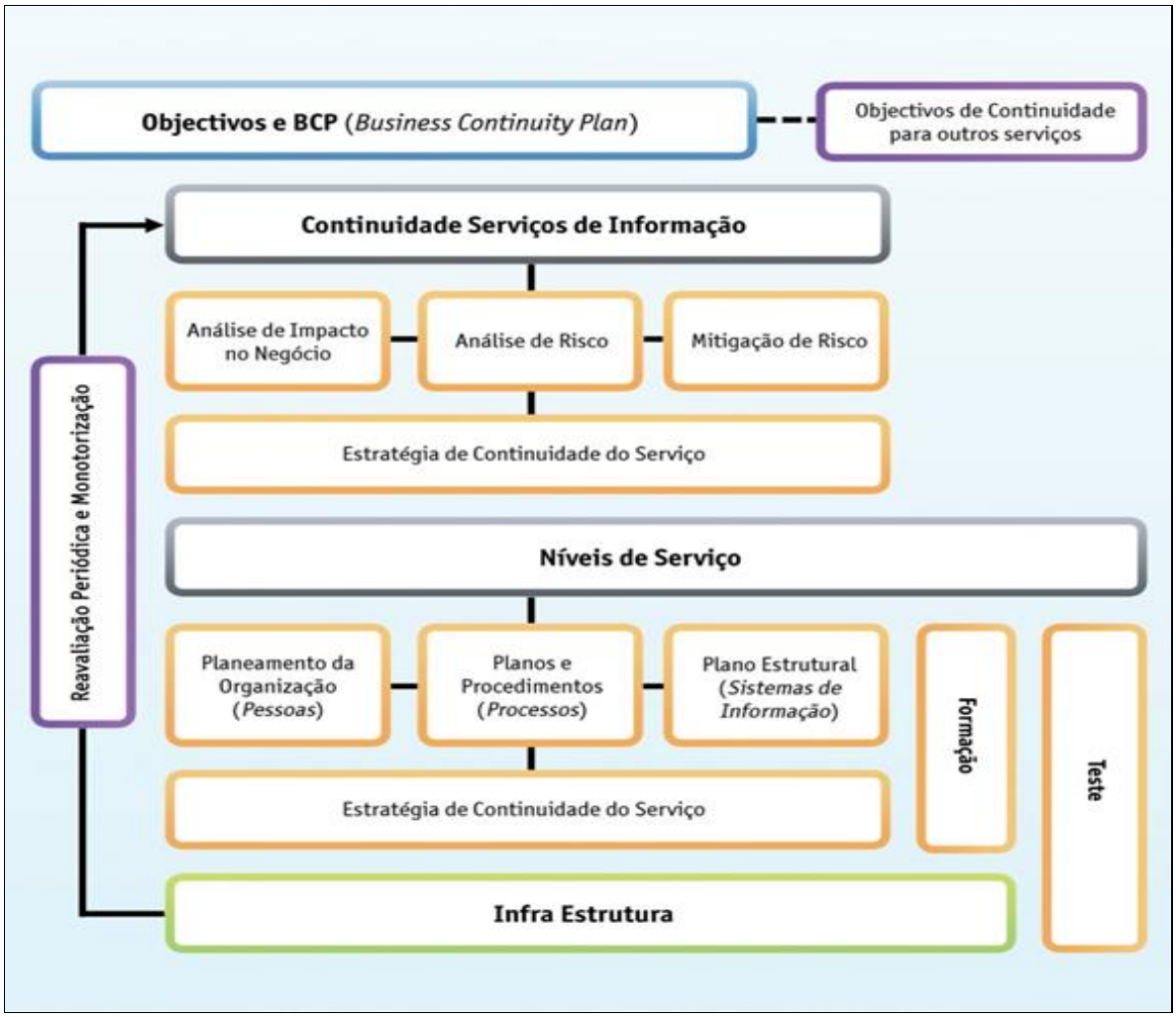


Figura 5 - Atividades Principais do Plano [17]

Quando se projeta um PCN deve-se considerar as seguintes etapas:

- Constatação da necessidade de elaborar o plano;
- Definir qual a equipa necessária para pôr em prática o plano;
- Definir planos alternativos na eventualidade de um desastre;
- Escrever o plano de recuperação de desastre e continuidade de negócio;
- Ensaiar o plano de recuperação de desastre e continuidade de negócio;
- Manter o plano de recuperação de desastre e continuidade de negócio devidamente atualizado;
- Implementar e avaliar o plano de recuperação de desastre e continuidade de negócio.

[17] Infosistema, 2010

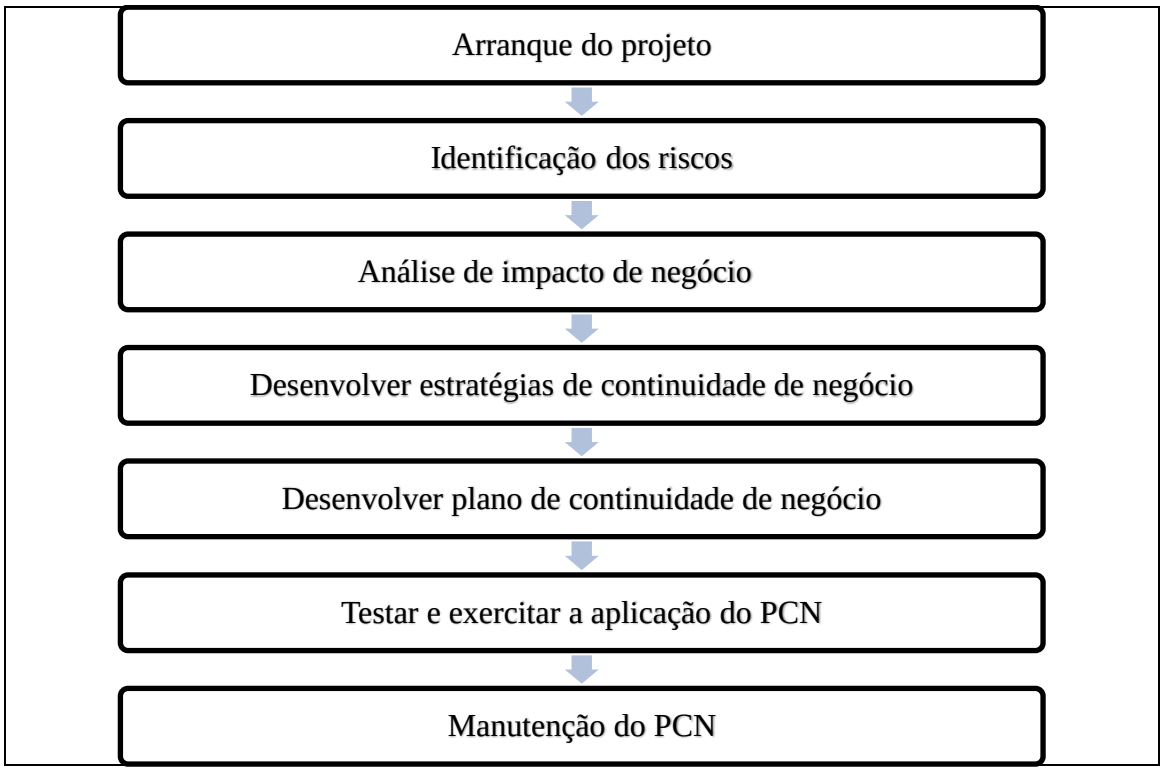


Figura 6 - Principais fases do BCM[18]

2.1.5.1 Identificação de Riscos/Análise de Impacto

É necessário elaborar uma análise dos riscos de forma a determinar as funções onde se verificam os impactos permitindo elaborar uma estratégia (Trindade, 2008), ou seja, é necessário elaborar uma análise de riscos que permita identificar os riscos na sua origem, para que depois seja possível, através da análise BIA identificar as funções críticas do negócio bem como a sua hierarquização.

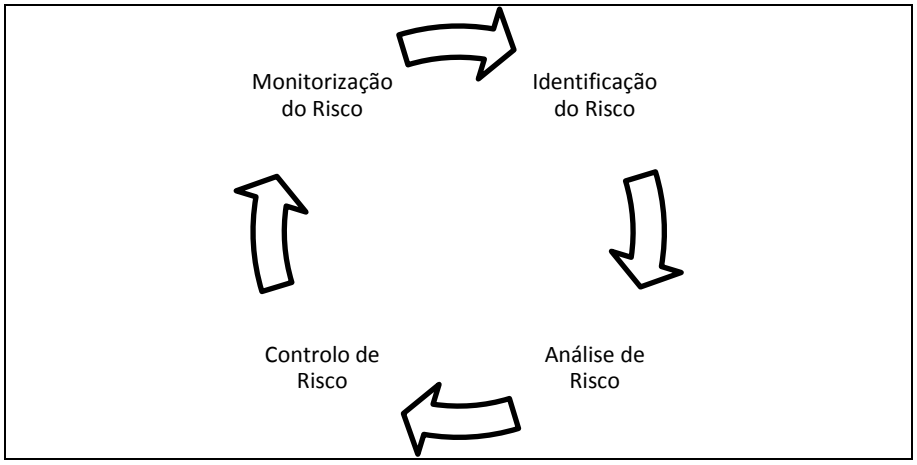


Figura 7 - Ciclo de Gestão de Risco[19]

[18] Gallagher, 2003, p. 5
[19] Gallagher, 2003, p. 9

A importância da análise de riscos é permitir obter uma relação dos ativos críticos, determinando-se os riscos e vulnerabilidades associados. Esta análise traz como benefícios imediatos: o conhecimento da real situação da organização, a identificação das medidas de segurança apropriadas, a melhor aplicação de recursos e a possibilidade de tomada de decisão baseada em factos reais.

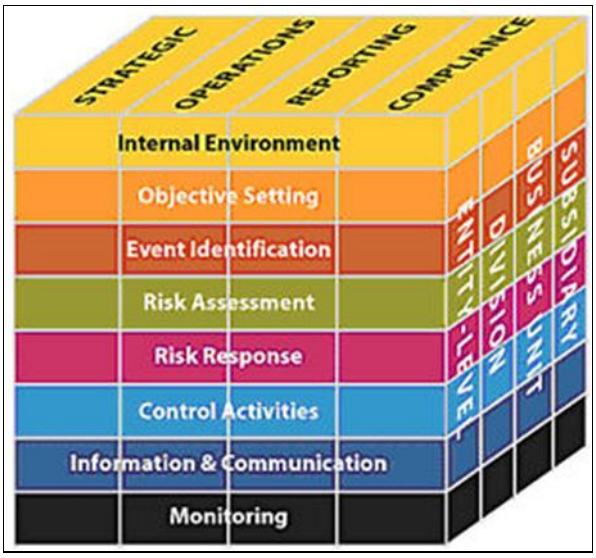


Figura 8 - Análise de risco dos processos de SI/TI[20]

De seguida descreve-se cada item das três faces da Figura 8 - Análise de risco dos processos de SI/TI

:

- Ambiente interno: aborda aspetos culturais da organização;
- Fixação de objetivos: os objetivos que se caracterizam pelas metas estratégicas definidas para a organização;
- Identificação de eventos: identifica os eventos internos e externos que podem influenciar o cumprimento dos objetivos estratégicos;
- Avaliação de riscos: análise quanto à probabilidade e o impacto dos riscos, de forma a estabelecer formas de gestão dos mesmos;
- Resposta a risco: delinear medidas para evitar, aceitar, reduzir ou transferir riscos;
- Atividades de controlo: definir e implementar políticas e procedimentos que possam assegurar resposta aos riscos identificados;

[20] Sinfic SA

- Informações e comunicações: identificar e recolher informação de forma a ser possível cumprir as responsabilidades no cumprimento da gestão dos riscos;
- Monitoramento: monitorizar as políticas e procedimentos através de avaliações periódicas e auditorias.

2.1.5.2 Estratégias de Recuperação de TI

Com os «*inputs*» da análise de risco e BIA é necessário descrever uma estratégia de forma a identificar as medidas mais eficientes na gestão de continuidade de negócio.

Através destas medidas é possível envolver decisões que determinem o tempo de recuperação de cada função crítica, face a uma avaliação de custo/benefício.

Nesta fase também se procede à definição da abordagem para recuperação das SI/TI.

Considerando a existência de vários tipos de estratégia de recuperação de TI, pode-se descrever, as mesmas, da seguinte forma:

«Hot-site» **-** Uma instalação de centro de dados ou instalação de escritório com *"hardware»* suficiente, interfaces de comunicação e espaço de ambiente controlado capaz de fornecer um sistema de *backup* imediato de apoio de processamento de dados. Os aplicativos podem ser balanceados e trabalhar com servidores ativos nos dois centros de processamento de dados, ou seja, em caso de indisponibilidade do centro de processamento de dados principal o utilizador do sistema não se apercebe da disrupção do serviço.

«Warm-site» – Aplica-se a sistemas com maior tolerância à paralisação, podendo estar sujeita à indisponibilidade por mais tempo até ser possível retomar a operacionalidade sem, no entanto, comprometer o serviço ou gerar impactos significativos. Os aplicativos trabalham com um ou dois centros de processamento de dados e são necessárias configurações.

«Cold-site» – Propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações. É aplicável apenas em situações em que a tolerância à indisponibilidade é muito grande. Para restaurar os aplicativos é necessário reinstalar todo o sistema, pois no centro de processamento de dados secundários existe apenas a infraestrutura de comunicação.

Tabela 2 - Seleção de critérios de site alternativo[21]

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

2.1.5.3 Implementação

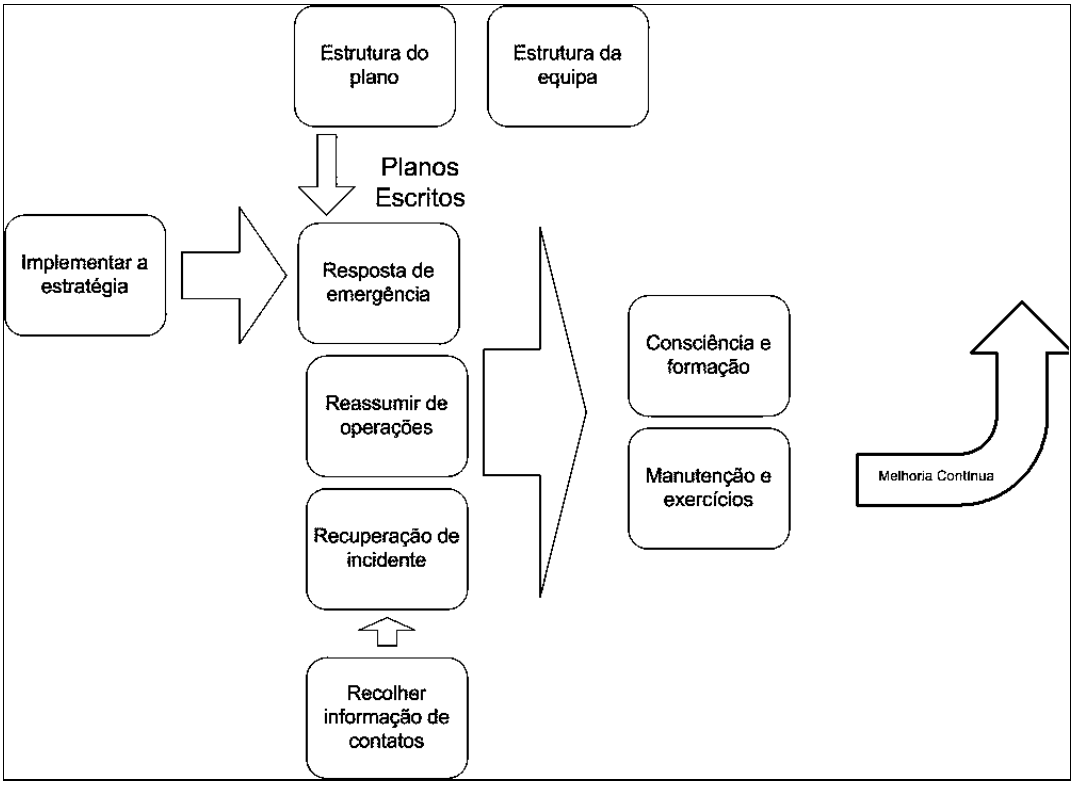


Figura 9 - Fase de implementação [22]

2.1.5.4 Gestão

Para que o plano se mantenha sempre atualizado é necessário definir um ator principal que se responsabilize por verificar e manter atualizado o plano através de verificações periódicas. Esse ator designa-se por Coordenador do plano de continuidade de negócio.

[21] Adaptado de Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002
[22] Adaptado de Trindade, 2008

2.1.5.5 Fases de Recuperação definidas pelo Plano de Continuidade Negócio

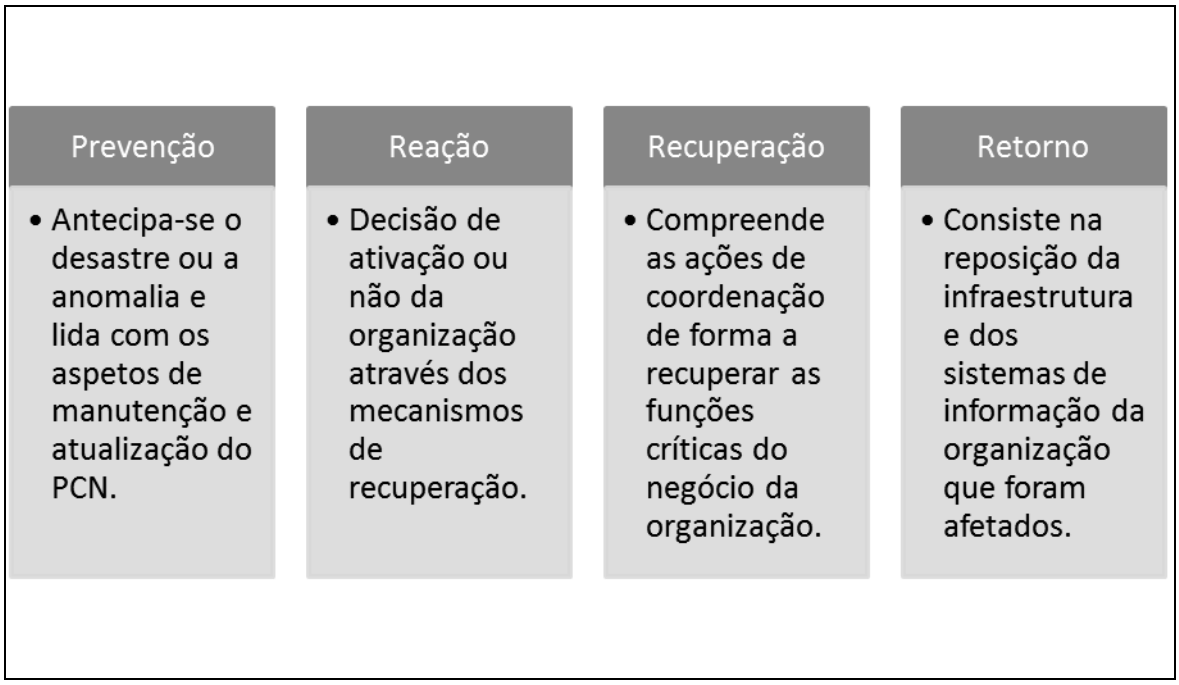


Figura 10 - Fases de Recuperação definidas pelo Plano de Continuidade Negócio

2.1.6 BENEFÍCIOS ESPERADOS DA CONTINUIDADE DE NEGÓCIO

Os benefícios associados ao plano de recuperação de desastre e continuidade de negócio são de diversas origens:

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

Os benefícios podem ser analisados a vários níveis:

- Operacional;
- Tático;
- Estratégico;
- Organizacionais;
- Económicas;
- Legais.

2.2 GESTÃO DE RISCO

Segundo diferentes autores a gestão de risco é cada vez mais um fator decisivo na estratégia de qualquer organização, considerando que existem cada vez mais variáveis: a globalização, nova era digital, complexidade dos produtos e serviços, leis reguladoras e o próprio mercado (The Institute of Risk Management *et al.*, 2002; Cavalcanti, 2009).

Segundo Gonçalves (2011) [23] o equilíbrio entre investimento em controlo e o nível de risco é fundamental para uma gestão, por considerar que os custos financeiros devem estar harmonizados com o nível de risco e a tolerância a esse risco, evitando a afetação de custos desnecessários. Gonçalves considera que a avaliação de riscos permite à Gestão de Topo a tomada de decisões relativas a investimentos em controlos que permitam a Organização manter-se no nível de risco que a mesma considera aceitável face aos riscos a que se encontra exposta.

Para Silva & Torres (2010)[24] a gestão de risco é uma peça fundamental para o planeamento de qualquer atividade é que sem esta peça podem ocorrer erros de planeamento de forma inexplicável. Silva *et al.* (2010) refere ainda que a gestão de risco deve ocorrer em todas as fases de um projeto, atividade, etc., consistindo num ciclo para a identificação das ameaças, qualificação do risco, redução do risco residual e aceitação formal do risco residual.

Segundo Carlos Cavalcanti (2009)[25] "…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."

Ao processo de gestão de risco está inerente uma prossecução de etapas:

- Identificação dos riscos necessária para análise quantitativa do risco, em que este é medido pelo impacto resultante da concretização da ameaça;
- Identificação das ameaças a que a organização está sujeita através da elaboração de cenários que facilitem a obtenção de informação estatística

[23] 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.
[24] Silva, P. T., & Torres, C. B. (2010). *Gestão e liderança para profissionais de TI.* Lisboa: FCA - Editora de Informática.
[25] Cavalcanti, C. D. (2009). Gestão de Riscos - Abordagem de conceitos e aplicações. Obtido em 10 de Abril de 2012, de Convergência Digital Blog publicado por Carlos Diego Cavalcanti Artigos e Análises: http://www.valcann.com/publicacoes/riscos_conceitosaplicacoes.pdf

sobre a frequência de ocorrência no passado que servirá para quantificar os riscos no passo seguinte;

- Identificação das vulnerabilidades que visa permitir o cálculo de probabilidade de concretização das ameaças a que a organização se encontra sujeita;
- Análise quantitativa permite quantificar ou qualificar a probabilidade das ameaças gerarem danos, numa análise de riscos.

Tabela 3 - Medição das consequências face às ameaças[26]

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.

Importa definir risco como qualquer situação que pode afetar a capacidade de alcançar objetivos, sendo intrínseca a qualquer atividade e decisão das organizações ou, como refere Cavalcanti (2009), risco pode ser considerado como "…ameaça de que um evento ou ação (interno ou externo) possa afetar negativa ou positivamente o ambiente no qual se está inserido".

O risco também pode ser descrito como "… a combinação da probabilidade de um acontecimento e das suas consequências" (A Risk Management Standard, 2002, p. 3).

Para Gonçalves (2011) o risco é uma opção e não uma inevitabilidade que deve ser tratado.

Existem autores que defendem que alguns gestores entendem a gestão de risco como um mal necessário, enquanto outros entendem a gestão de risco como uma origem de

[26] UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management, 2002, p. 8

oportunidades diferenciadoras, uma vez que não atuam só de forma preventiva aos eventos de incerteza, criam oportunidades de ganhos (Cavalcanti, 2009) (Gonçalves, 2011).

Gonçalves (2011) refere ainda que as organizações têm de ter uma cultura apropriada para a gestão de risco que deve ser estimulada pela Gestão de Topo em toda a organização, através da potenciação de motivação e envolvimento de todos os trabalhadores.

Acresce referir que a gestão de risco difere nas suas características específicas em função do sector de atividade em estudo, que no caso desta dissertação se enquadra fundamentalmente na categoria dos riscos dos sistemas de informação e tecnologias de informação.

O risco específico consiste na probabilidade de ocorrerem impactos negativos, decorrentes da inabilidade dos sistemas de informação e tecnologias de informação de impedir acessos não autorizados, assegurar a integridade dos dados e garantir a continuidade do negócio em caso de falha.

Gonçalves (2011) considera que de acordo com o Modelo de Avaliação de Risco (MAR) existem cinco classificações de risco, relativamente aos riscos de sistemas de informação:

- Risco de estratégia, que resulta dos riscos associados à inadequação da estratégia e politicas definidas;
- Risco de flexibilidade, que resulta dos riscos associados à complexidade e inflexibilidade dos sistemas de informação;
- Riscos de acesso, que decorrem dos riscos associados aos acessos não autorizados;
- Riscos de integridade, que derivam dos riscos associados à qualidade da informação produzida pelo sistema de informação;
- Risco de continuidade, que advêm dos riscos associados às falhas operacionais.

Em suma, a gestão de risco pode ser descrita como um processo de identificação e avaliação de risco e, como um meio para se tomarem medidas preventivas, de forma a reduzir o risco a um nível considerado aceitável. O principal objetivo da gestão de risco é proteger a organização e a capacidade desta realizar a sua missão uma vez que permite que os gestores tomem decisões de gestão de risco bem informados de forma a justificar os custos que fazem parte de um orçamento de TI. A gestão de risco deve ser considerada como uma função essencial na gestão da organização.

2.2.1 BENEFÍCIOS DA GESTÃO DE RISCO

Cavalcanti (2009) elenca alguns benefícios após a implementação integrada de uma gestão de riscos, tais como:

- Ter uma visão estruturada dos processos de negócio;
- Permitir que os gestores possuam as melhores ferramentas de controlo face à incerteza do contexto organizativo;
- Determinar a possibilidade de perda de informação perante os riscos;
- Permitir a identificar situações de recuperações de dados;
- Possibilitar a eliminação de fontes de riscos, transformando-as em oportunidades;
- Garantir a continuidade de negócio;
- Estruturar a cadeia de valor, das condições interna e externas no mercado em que a organização se insere;
- Organizar a interpretação dos potenciais aspetos positivos e negativos de todos os agentes que possam afetar a organização;
- Diminuir a indeterminação em relação ao alcance de todos os objetivos globais da organização;
- Diminuir a probabilidade de insucesso.

2.2.2 DICIONÁRIO DE RISCOS

O dicionário de riscos funciona como um catálogo, com as derivações possíveis e particulares de risco de cada segmento relativo ao negócio da organização. Este dicionário tem como objetivo prover o direcionamento das ações de gestão de riscos e processos contidos na cadeia de valor do negócio[27], bem como as condições interna e externas do mesmo (Cavalcanti, 2009).

[27] "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 11 - Cadeia de valor de riscos e processos, considerando as condições externas e internas[28]

2.2.3 METODOLOGIA

Das várias normas que existem para gestão de riscos considerou-se o Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002) como o mais relevante para o presente estudo por descrever uma metodologia de gestão de risco baseada em todas as fases do ciclo de vida de desenvolvimento de sistema[29].

Como referido anteriormente a gestão de risco deve ser totalmente integrada no SDLC e é aplicada da mesma forma independente da fase do SDLC em que o processo se encontra. Como é referido por Stoneburner *et al.* (2002, p. 4) o SDLC de um sistema apresenta cinco fases distintas:

1. Iniciação – os riscos identificados nesta fase são usadas para apoiar o desenvolvimento de requisitos de sistema, incluindo os requisitos e estratégia de segurança;

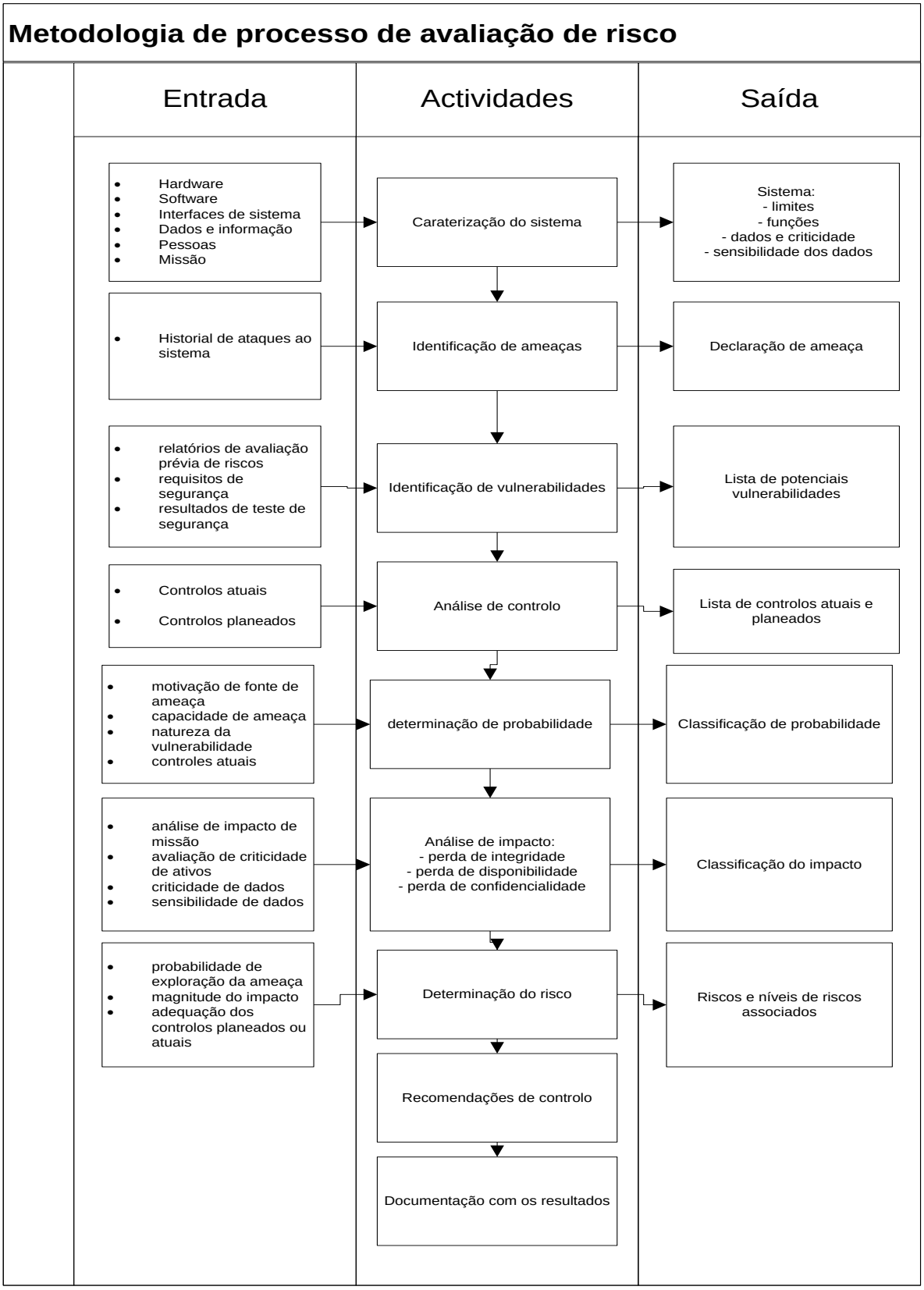
[28] Cavalcanti, 2009, p. 10
[29] SDLC

2. Desenvolvimento ou aquisição - Os riscos identificados durante esta fase podem ser usados para apoiar as análises de segurança do sistema podendo levar a alterações desenho e arquitetura durante o desenvolvimento do sistema
3. Implementação – Nesta fase é prestada o suporte à avaliação da implementação do sistema considerando as suas necessidades dentro de seu ambiente operacional modelado.
4. Operação ou manutenção – todos os riscos devem ser identificados antes desta fase. Todas as atividades de manutenção devem ser executadas de forma periódica ou sempre que ocorram grandes mudanças no ambiente operacional, isto é, no ambiente de produção do sistema.
5. Eliminação – esta fase é executada para componentes de *"hardware»* e *«software»* do sistema que serão eliminados ou substituídos para que se tenha a garantia que os mesmos são devidamente eliminados, e que qualquer dado residual obtém tratamento adequado de forma a reduzir ou eliminar qualquer risco.

A avaliação de risco é a primeira fase da metodologia de gestão de risco proposta por por Stoneburner *et al.* (2002, p. 4). Esta fase serve para determinar potencial grau de ameaça e o risco associado com um sistema de TI durante todo seu SDLC. O relatório resultante desta análise identifica possíveis controlos que reduzam ou eliminem o risco.

A avaliação de risco pressupõe a existência de 9 atividades.

Tabela 4 - Metodologia de processo de avaliação de risco[30]



[30] Adaptado de Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002

Na primeira atividade é feita a caraterização do sistema que pressupõe a definição do âmbito do esforço de avaliação de risco, delimitando os limites operacionais de autorização e fornecendo informações: «*hardware*», «*software*», interfaces de conectividade de sistema interna e externas, dados e informação, pessoal responsável da divisão ou suporte, missão do sistema, valor ou importância que o sistema tem na organização, nível de proteção requerida para manter a integridade confidencialidade e disponibilidade do sistema, requisitos funcionais do sistema, políticas de segurança, arquitetura de sistema, topologia de rede, informações das políticas de armazenamento que protegem a confidencialidade, integridade e disponibilidade de dados e sistemas, segurança física do ambiente físico; essenciais para definir o risco.

Na segunda atividade é feita a identificação de ameaças.

Relativamente ao conceito de ameaça[31] o autor João Luiz Pereira Marciano (2006) refere que das pesquisas que realizou é possível categorizar as ameaças, conforme se lista a seguir:

1. Ameaças naturais: inundações, terramotos, tornados, deslizamentos de terra, avalanches, tempestades elétricas, etc.
2. Ameaças humanas:
    a. Eventos deliberados cometidos com o uso de «*software*»,
    b. Erros ou falhas técnicas de *«software»* (falhas de codificação, «*bug*»);
    c. Falhas ou erros humanos (acidentes, enganos dos empregados);
    d. Atos deliberados de espionagem ou invasão, *hacking*;
    e. Atos deliberados de sabotagem ou vandalismo (destruição de sistemas ou informação);
    f. Atos deliberados de furto;
    g. Atos deliberados de extorsão de informação.
3. Ameaças de ambiente:
    a. Falhas elétricas de longo prazo;
    b. Poluição;
    c. Erros ou falhas técnicas de «*hardware*»;
    d. Etc.

[31] Incidente ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso informático e, portanto, as informações a ele ligadas.

Tabela 5 - Probabilidade de ocorrência de ameaças [32]

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.

Na terceira atividade é feita a identificação de vulnerabilidades. Vulnerabilidade é definida como fraqueza ou deficiência que faz com que uma determinada ameaça ocorra, isto é, representa um ponto potencial de falha ou um elemento relacionado à informação que é possível de ser observado por alguma ameaça.

Para a identificação de vulnerabilidades pode-se utilizar ferramentas como listas de verificação e ferramentas de *«software»* que determinam as vulnerabilidades, conforme Tabela 6 - Lista de critérios de segurança para identificação de vulnerabilidades.

[32] UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management, 2002, p. 8

Tabela 6 - Lista de critérios de segurança para identificação de vulnerabilidades [33]

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;

[33] Adaptado de Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002

O objetivo da quarta atividade, segundo Stoneburner *et al.*. (2002), é analisar os controlos que foram implementados ou estão planeados para implementação, pela organização para minimizar ou eliminar a probabilidade de uma ameaça exercer uma vulnerabilidade no sistema.

Stoneburner *et al.*. (2002) referem que a atividade cinco tem como objetivo permitir obter uma classificação geral de probabilidade que indica a probabilidade de que uma vulnerabilidade potencial poderá ser exercida dentro de determinado ambiente de ameaça, considerando os seguintes fatores:

- Capacidade e motivação da fonte da ameaça
- Natureza da vulnerabilidade
- Existência e eficácia dos controlos atuais.

A probabilidade de que uma potencial vulnerabilidade pode ser descrita como alta, média ou baixa, conforme Tabela 7 - Classificação geral de probabilidade

Tabela 7 - Classificação geral de probabilidade [34]

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.

A sexta atividade é análise de impacto (BIA)[35]. Esta atividade permite determinar os efeitos adversos resultantes do exercício bem-sucedido de uma ameaça/vulnerabilidade (Stoneburner, Goguen, & Feringa, 2002).

A sétima atividade é a determinação de risco. A finalidade desta etapa é avaliar o nível de risco para os diversos sistemas. Segundo Stoneburner *et al*. (2002) a determinação do risco para um par ameaça/vulnerabilidade específico pode ser expressa como uma função: da probabilidade de uma determinada fonte de ameaça a tentar exercer uma determinada vulnerabilidade; da magnitude do impacto deve com sucesso uma ameaça-fonte exercer a

[34] Adaptado de Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, & Feringa, 2002)
[35] Capítulo 2.4 página 48

vulnerabilidade e da adequação dos controlos de segurança existentes ou planeados para reduzir ou eliminar o risco.

Para medir o risco, devem ser desenvolvidas uma escala de risco e uma matriz de risco-nível (Stoneburner, Goguen, & Feringa, 2002), conforme Tabela 8 - Tabela resumo das categorias de impacto no negócio.

Pode-se classificar os níveis de impacto nas seguintes categorias:

Tabela 8 - Tabela resumo das categorias de impacto no negócio[36]

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

Pode-se classificar o impacto do negócio em quatro subcritérios, cada um com um peso diferenciado, na organização (Alves, 2009, p. 7):

- Imagem – Peso 4;
- Financeiro – Peso 3;
- Legislação – Peso 2;
- Operacional – Peso 2.

O valor numérico atribuído a cada peso foram os seguintes:

- Extremamente com o valor numérico de 9,25 corresponde ao peso 5;
- Bastante com o valor numérico de 7,08 corresponde ao peso 4;
- Medianamente com o valor numérico de 4,62 corresponde ao peso 3;

[36] Adaptado de Ferrer

- Pouco com o valor numérico de 2,27 corresponde ao peso 2;
- Nada com o valor numérico de 0,54 corresponde ao peso 1.

Stoneburner *et al.* (2002) referem que na oitava atividade são indicados os controlos que poderiam atenuar ou eliminar os riscos identificados, reduzindo o nível de risco para um nível aceitável.

Por fim, Stoneburner *et al.* (2002) referem que no final do processo de gestão de risco todos os resultados devem ser compilados num único relatório oficial cujo objetivo é ajudar os membros da administração e os gestores a tomar decisões do foro politica, processual, orçamental, operacional e de gestão.

Para além desta metodologia existem ainda as seguintes normas para a gestão de risco:

- A norma ISO 31000 (Wikipedia, 2012) foi publicada em 13 de novembro de 2009 e referencia um padrão para a implementação de gestão de risco, podendo ser aplicada a qualquer entidade pública ou privada, qualquer que seja a sua atividade ou negócio de forma a proporcionar a melhor estrutura prática e orientação para todas as operações em causa com a gestão de risco.
- A norma ISO 31000:2009 fornece diretrizes genéricas para a conceção, implementação e manutenção de processos de gestão de riscos em toda a organização.
- A ISO 31000 define risco como o "…efeito de incerteza sobre os objetivos..." Esta norma define o contexto interno e externo de uma organização, monitoriza e revê todas as atividades do processo de gestão de risco comunicando com todos os proprietários de risco envolvidos na gestão de risco (Mrasmussen, 2009).
- A norma ISO 27005:2008 (Portal, 2008) abrange gestão de riscos de segurança de informação. A norma fornece diretrizes para a gestão de riscos de segurança de informações numa organização, especificamente para suportar os requisitos dum sistema de gestão de segurança de informação definido pela ISO 27001, sendo aplicável a todos os tipos de organização.

2.3 ANÁLISE RISCO

Silva *et al.* (2010) referem que a análise de risco é um processo que tem como propósito produzir informação de forma sistemática para determinar o grau de exposição da

organização aos diversos riscos a que está sujeita permitindo Gestor de Topo suportar a tomada de decisão em matéria de controlos de segurança a implementar.

A análise de risco propõe-se a detetar os ativos da organização, as ameaças e vulnerabilidades desses ativos, encontrando pontos frágeis dos SI, de modo a evitar investimento em segurança desnecessário, permitindo a implementação consistente de medidas de segurança.

O objetivo principal de realizar uma análise de risco é fornecer à administração e liderança, uma visão clara da situação atual, para prestar apoio na tomada de decisões.

A análise de risco permite identificar os eventos que estão a ocorrer ou possam vir a acontecer e determinar o seu impacto na organização.

Uma análise de riscos deve ser realizada antes de a organização iniciar um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou até mesmo uma relação de parceria.

O processo de análise de riscos deve envolver especialistas em análise de riscos e especialistas no negócio da organização.

Tipicamente a análise de risco deve ser realizada no menor tempo possível considerando que a organização é assente numa estrutura dinâmica.

O risco tem três elementos:

- Evento
- Probabilidade
- Impacto

O risco pode ser dividido em risco de negócio e risco operacional.

O risco de negócio geralmente está associado a fatores externos à organização, como, por exemplo, os aspetos econômicos, competitivos, legais, etc. Este tipo de análise suporta a tomada de decisões no plano estratégico da Organização.

O risco operacional está associado às operações que ocorrem internamente na organização.

O risco pode ser classificado em cinco categorias, conforme Tabela 9 - Fontes típicas de risco, por categoria:

Tabela 9 - Fontes típicas de risco, por categoria[37]

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

[37] Adaptado de Nakashima & Carvalho, 2004

2.3.1 METODOLOGIA DA ANÁLISE DE RISCO

Existem formas de realizar a análise de risco que podem ser integradas para melhorar os resultados, de forma independente:

- Análise de Processo[38]: Consiste em analisar os processos, incluindo os controlos para a gestão de riscos do ponto de vista do «*design*», permitindo chegar às conclusões de problemas endêmicos que se repetem ao longo do tempo;
- Análise Técnica[39]: Trabalha sobre os ativos e suas configurações, tentando determinar desvios dos padrões estabelecidos;
- Conjunto Análise[40]: Após uma revisão dos processos e respetivas formas/mecanismos de controlos, para aqueles que são adequados, uma verificação técnica é feita para corroborar os resultados.

A concretização de uma Análise de Risco fornece um documento indicador que dá à organização o controlo sobre a sua estratégia, considerando que com este relatório pode-se identificar os controlos que devem ser executados em curto, médio e longo prazo.

A Norma de Gestão de Risco (A Risk Management Standard, 2002) refere que é importante apresentar os riscos de forma estruturada e para o efeito concebeu a Tabela 10 - Descrição dos riscos, cuja finalidade é facilitar a descrição dos riscos e sua avaliação.

[38] Por exemplo, o Gestor de rede pode fazer alterações sem controlo associado
[39] Por exemplo, problemas de configuração de «*firewall*»
[40] Por exemplo, existem controlos de mudança na rede e na análise dos dispositivos é suficiente

Tabela 10 - Descrição dos riscos[41]

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

Para António Brasiliano[42] é na análise de risco que se estabelecem os critérios importantes para os dois parâmetros: a Probabilidade e o Impacto. O cruzamento destes dois parâmetros tem como resultado uma Matriz de Riscos (Figura 12 – Exemplo Matriz Impacto x Magnitude - Análise de Riscos).

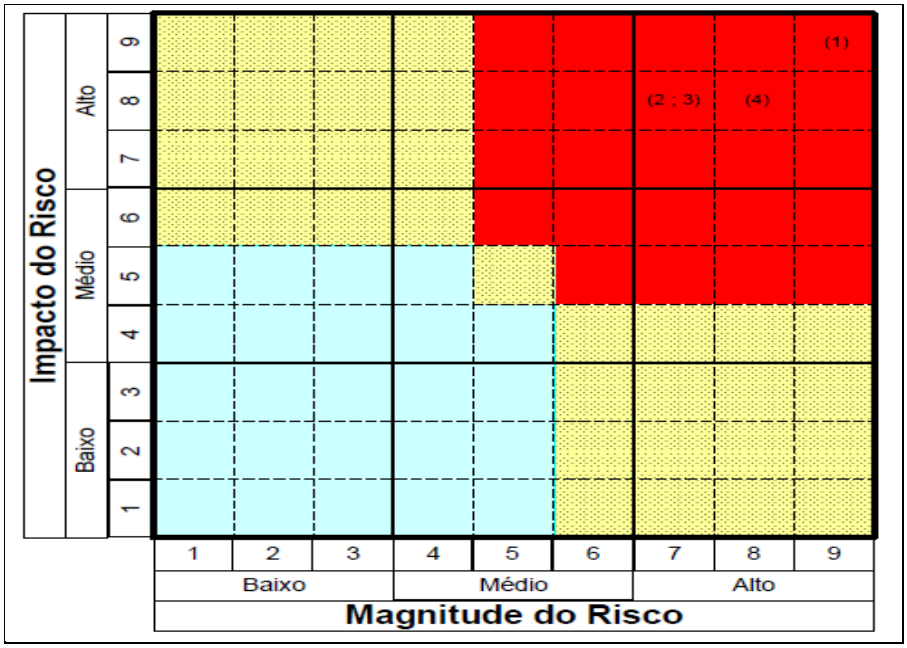


Figura 12 – Exemplo Matriz Impacto x Magnitude - Análise de Riscos

[41] A Risk Management Standard, 2002, p. 7

[42] Brasiliano, A. C. (março de 2009). *Método avançado de análise de risco.* Obtido em 19 de agosto de 2012, de Blog da Brasiliano & Associados:http://www.brasiliano.com.br/pdf/metodo_avancado_de_analise_de_riscos.pdf

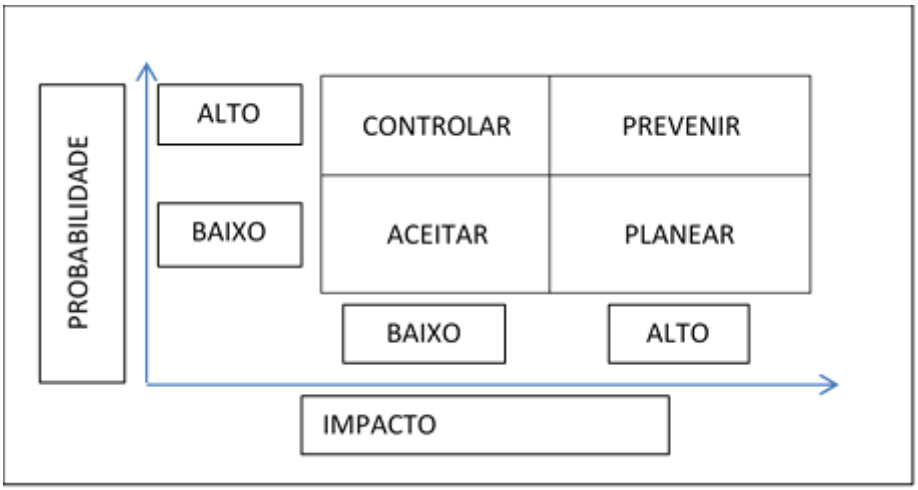


Figura 13 - Matriz de Risco[43]

De forma resumida, pode-se depreender da Figura 12 – Exemplo Matriz Impacto x Magnitude - Análise de Riscos e da Figura 13 - Matriz de Risco, que o gestor tomará decisões corretivas mediante a análise da métrica Magnitude x Impacto e tomará decisões preventivas mediante a análise da métrica [(Magnitude x Impacto) x Probabilidade].

Um dos modelos de risco utilizados é o *Project Management Body of Knowledge* (PMBoK) (Project Management Institute, 2004). O *PMBoK* é um conjunto de práticas em gestão de projetos, publicado pelo *Project Management Institute* (PMI) e constitui a base do conhecimento na gestão de projetos do PMI. Estas práticas são compiladas na forma de um guia, chamado de o Guia *PMBoK* (WIKIPEDIA, 2012).

2.3.2 PRINCIPAIS NORMAS

- BS ISO 31100 - Gestão de riscos. Código de boas práticas e orientações para a aplicação da BS ISO 31000 - Descreve o processo de gestão de risco que pode ser seguido e interpretados de modo que cada grupo trabalha de uma forma que é apropriada para eles e vai aumentar a consistência e a comunicação na organização (British Standards Institution, 2011);
- ISO 27005 - é o nome da série «*standard*» principal 27000 cobrindo informação de gestão de riscos de segurança. Esta norma fornece orientações para a informação de gestão de riscos de segurança numa organização, especificamente apoiar os requisitos de um sistema de gestão de informações de segurança definido pela ISO 27001.

[43] Adaptado de Gallagher, 2003, p. 47

- COBIT 5 - é um «*framework*» de negócios para governança e gestão de TI. Esta versão incorpora as últimas novidades em governança corporativa e técnicas de gestão. Fornece princípios globalmente aceites, práticas, ferramentas e modelos analíticos para ajudar a aumentar a confiança e valor nos sistemas de informação (Fagundes E. M., 1996-2012);
- ISO 27002 - A norma ISO 27002 é a renomeação da norma ISO 17799, e é um código de práticas para segurança da informação. Descreve centenas de controlos e mecanismos potenciais de controlo, que podem ser implementados, em teoria, sujeitos à orientação fornecida na ISO 27001. A norma também se destina a fornecer 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 - Propõe um sistema modular que complementa tanto a abordagem do processo como a abordagem técnica dando assim uma visão mais completa e precisa do estado da arte da segurança de TI[44];
- ISO/IEC 17799/2003[45] – A norma é um conjunto de recomendações para práticas na gestão de Segurança da Informação. A ISO/IEC-17799/2003 tem como objetivos: confidencialidade, integridade e disponibilidade das informações, os quais são fatores muito importantes para a segurança da informação. Para além das características indicadas atrás, esta norma inclui ainda as seguintes características: legalidade, responsabilidade, autenticidade, autoridade, não repúdio e auditoria.

2.4 ANÁLISE OU AVALIAÇÃO DE IMPACTO DE NEGÓCIO[46]

A análise de impacto de negócio ou avaliação de impacto de negócio (análise BIA) pode ser descrito como um processo de negócio e é a primeira etapa de um plano BCP.

A análise BIA é uma avaliação direta e objetiva do impacto financeiro que a organização vai sofrer face a uma falha da operação dos serviços de TI.

[44] Wikipedia. (12 de Fevereiro de 2012). ITILv3. Obtido em 14 de Agosto de 2012, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ITILv3
[45] Wikipedia. (27 de Dezembro de 2011). ISO/IEC 17799. Obtido em 14 de Agosto de 2012, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ISO/IEC_17799
[46] BIA

George Wrenn[47] refere-se à análise BIA como um processo analítico que tem como objetivo revelar negócios e impactos operacionais decorrentes de qualquer número de incidentes ou ocorrências.

Sandra Alves[48] refere, que segundo Antonio Celso Ribeiro Brasiliano[49], a análise BIA permite ter uma visão estratégica de continuidade, dando prioridade aos processos de negócio mais relevantes da empresa em nível de impacto no negócio e em nível de tolerância, para só então partir para o planeamento dos procedimentos de contingência e obter uma definição mínima dos componentes que tenham de ser replicados.

Assim sendo, pode-se definir a análise BIA como um processo linear que consiste em técnicas e metodologias que podem ser usadas para identificar, quantificar e qualificar o impacto e seus efeitos da perda de uma interrupção de negócios, em número de dias, e do ponto de vista financeiro, ou seja, definir qual é o tempo razoável para a organização recuperar de determinada disrupção no negócio e desempenhar as suas operações normalmente (California Emergency Management Agency, 2011) (Pelant, 2005).

No contexto do presente estudo, isto é, TI/SI a análise BIA permitirá determinar os sistemas de aplicativos críticos de tempo, dados e telecomunicações e determinar o tempo de recuperação e os objetivos de ponto recuperação, na organização.

No fundo, a análise BIA, vai permitir que a organização meça os riscos a que está sujeita contra os impactos, de forma a determinar onde a organização deve concentrar o seu tempo, esforço e investimento, ou seja, determinar onde e como a organização deve despender o que tem orçamentado para continuidade de negócio.

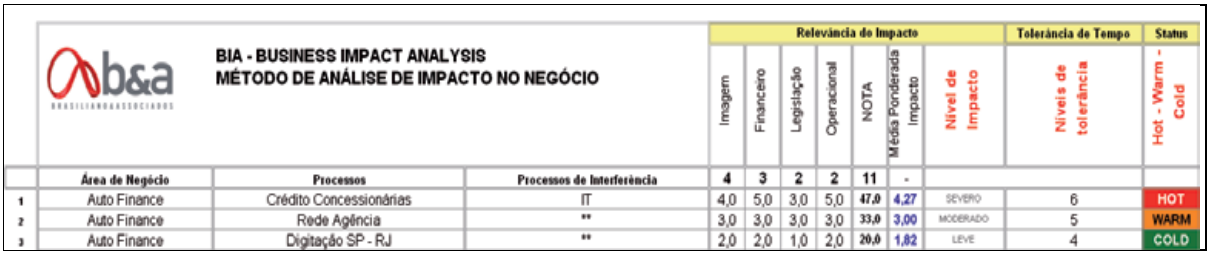
Para realizar a análise BIA é necessário o correto entendimento dos processos de negócio e a real influência que eles sofrem pelos serviços de SI/TI, ou seja, é necessário conhecer de forma detalhada todas as operações de negócios da organização.

O objetivo de mapear a importância dos processos críticos é priorizar a sua recuperação, tendo sempre em vista em vista o impacto no negócio e o tempo de tolerância (Alves, 2009).

[47] George Wrenn, C. (2000-2012). Obtido em 23 de fevereiro de 2012, de Information Security information, news and tips - SearchSecurity.com: http://searchsecurity.techtarget.com/#

[48] Alves, S. (abril de 2009). ANÁLISE Critérios e Parâmetros para Realização do Bia - Business Impact Analysis - no PCN. *GESTÃO de RISCOS*

[49] Diretor executivo da Brasiliano & Associados Gestão de Riscos Corporativos



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 14 - Exemplo de um ficheiro com análise BIA[50]

A análise BIA toma particular relevância considerando que permite dar resposta às seguintes perguntas: Quais os riscos associados ao negócio? Os riscos podem ser quantificados? Quais as medidas que têm de ser considerados para que o negócio prevaleça funcional em caso de desastre?

Quando se elabora uma análise BIA é necessário identificar as seguintes variáveis:

a) Datas criticas e impacto na linha temporal, isto é, identificar datas criticas para o negócio e o quanto tempo o negócio demoraria a sentir o efeito de uma paragem nesses momentos;

[50] Alves, 2009 página 8

Pode-se classificar os níveis de tolerância ao tempo de acordo com a seguinte tabela:

Tabela 11 - Relação do nível de tolerância/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 escala da Tabela 11 - Relação do nível de tolerância/tempo é o utilizado no capítulo 2.1.1.2 Impacto versus probabilidade, página 20.

b) Impactos operacionais e financeiros:
   - É necessário descrever os impactos nas operações especificando os custos financeiros associados em caso de interrupção da atividade em determinado processo.

c) Dependências:
   - Lista de todos os componentes em que os processos assentam para serem garantidos sem interrupções.
   - As dependências podem ser internas ou externas.

d) Recuperação de tempo objetivo [51]

e) Procedimentos alternativos:
   - Para cada procedimento alternativo deve-se identificar os seguintes dados: nome do procedimento, descrição, última data de utilização ou teste, *«hardware»* necessário, pessoal adicional necessário, tempo de utilização, tempo de implementação e respetivo custo.

[51] RTO - Período a partir do qual todos os dados e serviços críticos têm de estar operacionais. Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a organização determina por "perda aceitável" numa situação de desastre. O RPO permite que a organização defina uma janela de tempo, antes que um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais

2.4.1 ELEMENTOS CHAVE DA ANÁLISE BIA

Figura 15 - Elementos chave da análise BIA[52]

[52] Adaptado de Estall, 2010

De forma sucinta descreve-se cada um dos elementos da Figura 15 - Elementos chave da análise BIA

:

- Identificar todas as instalações físicas da organização;
- Obter a lista de processos que são executados em cada instalação e determinar quais as que se relacionam de direta ou indiretamente com o serviço, isto é, identificar os processos e respetivas dependências;
- Analisar a criticidade de cada processo em cada instalação, isto é descrever a importância de cada um dos processos;
- Estimar através de inquéritos ou entrevistas o RTO, RPO e MTD para cada processo de instalação;
- Imposição de processos crítica a cada instalação, considerando as criticidades impactos para os negócios, RTO, RPO e MTD.

2.4.2 METODOLOGIA

A análise BIA deve ser considerada como um projeto de curta duração que englobe as seguintes fases: planear, recolha de dados, análise de dados, elaboração de relatório e aceitação da gestão de topo (Pelant, 2005).

Tabela 12 - Metodologia de análise BIA [53]

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

[53] Adaptado de Pelant, 2005

<table>
<tr><th colspan="5">Metodologia de análise BIA</th></tr>
<tr><th>Fase</th><th colspan="4">Descrição</th></tr>
<tr><td rowspan="5">Dados</td><td rowspan="4">Preparar a estratégia de recolha de dados</td><td>Identificar os participantes</td><td colspan="2">• Representantes de cada área funcional
• Representante da Gestão de Topo</td></tr>
<tr><td rowspan="3">Determinar a abordagem</td><td>Entrevista</td><td>• Desenvolver guião de entrevista
• Treinar entrevistadores
• Validar guião</td></tr>
<tr><td>Questionário</td><td>• Definir a estrutura do questionário
• Desenvolver o processo de análise de dados
• Desenvolver as instruções
• Validar questionário</td></tr>
<tr><td colspan="2">Combinação dos dois métodos</td></tr>
<tr><td>Desenhar a infraestrutura</td><td colspan="2">• Missão
• Principais objetivos
• Organização
• Dependências
• Impactos de interrupções ao longo do tempo
• Potencial de mitigação de impacto</td></tr>
<tr><td rowspan="2">Realizar a recolha de dados</td><td>Preparar os participantes</td><td colspan="2">• Emitir comunicado com objetivos
• Apresentação Formal dos procedimentos
• Distribuir as diretrizes da entrevista/agendamento de entrevistas ou distribuir o questionário
• Indicar tempo de conclusão</td></tr>
<tr><td>Recolher dados</td><td colspan="2">• Entrevista
• Questionário</td></tr>
</table>

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[54]: o Perda de receitas o Custo de sanções e multas • Qualitativa[55]: 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	

[54] Perdas ou despesas extra que são quantificáveis em termos financeiros
[55] Impactos operacionais ou intangíveis que não são quantificáveis em termos financeiros

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

Rodrigo Ferrer[56] refere que, de acordo com o Business Continuity Institute, os quatro objetivos principais da análise BIA são:

- Identificar os processos críticos que suportam a atividade da organização e a prioridade de cada um dos serviços e os RTO;
- Determinar o tempo máximo tolerável de inatividade[57];
- Apoiar o processo para identificar as melhores estratégias de recuperação.

Para Doug Stoneman[58] a melhor prática da análise BIA é determinar os seguintes pontos:

- Identificar os custos financeiros e não financeiros;
- Estabelecer cada janela de tempo em que a recuperação tem de ocorrer;
- Identificar *«software»*, *«hardware»*, sistemas e dados críticos;
- Produzir uma avaliação dos recursos necessários para a recuperação e continuação do negócio;

[56] Ferrer, R. (s.d.). *Continuidad del negocio.* Obtido em 23 de Fevereiro de 2012, de SISTESEG COLOMBIA: http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.pdf

[57] MTD – Tempo máximo tolerável de inatividade (Maximum Tolerable Downtime) - Especifica o período máximo de tempo que um determinado processo empresarial pode estar inoperante antes de a sobrevivência da organização estar em risco

[58] Stoneman, D. (Dezembro de 2003). Business Continuity and Business Impact Analysis (BIA) Best Practices. The Issa Journal, p. 4.

- Fornecer dados sobre os riscos do negócio que possam não ter sido identificados anteriormente;

Para atingir estes objetivos é necessário examinar os processos críticos, realizar questionários e entrevistas, rever processos chaves e fluxos de processo (Stoneman, 2003).

2.4.4 BENEFÍCIOS

Segundo Chip Cleary[59] a análise BIA apresenta os seguintes benefícios:

- Estima os benefícios da aprendizagem, expressos em valores em euros;
- Permite a gestão de dados de forma a tornar claro o âmbito decisões;
- Fornece às equipas de formação diretrizes concretas sobre o âmbito da formação;
- Trabalha mesmo em situações onde existem vários fatores de impacto;
- Serve de suporte para a melhoria contínua, o que permite aos grupos responsáveis pela formação ajustar de forma continua a formação.

2.4.5 EXEMPLOS DE ATIVIDADES CRÍTICAS

Swanson *et al.*[60] identifica os seguintes recursos como críticos no suporte dos processos de negócio:

- Autenticação dos utilizadores, isto é, acesso à rede local;
- Servidor de base de dados;
- Servidor e serviço de correio eletrónico;
- Computadores dos utilizadores;
- *«HUB»*;
- Rede;
- Eletricidade;
- Aquecimento, ventilação e ar condicionado;
- Segurança física;
- Impressão.

[59] 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 2012, de MediaTec Publishing Inc: http://clomedia.com/articles/view/measuring_business_results_using_business_impact_analysis

[60] 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.

3 METODOLOGIA DE PESQUISA

A elaboração de um plano de continuidade de negócio envolve a preparação, teste e manutenção de ações específicas para proteger os processos críticos da organização[61].

Para que cada organização possa catalogar seus sistemas críticos e definir um tempo máximo de interrupção para cada um destes serviços é necessário elaborar uma análise BIA.

Segundo Sousa & Baptista (2011, p. 53) entende-se por metodologia de investigação todo o processo de seleção da estratégia de investigação, com o qual se pretende atingir um ou mais fins. A escolha da metodologia depende do fim que se pretende atingir.

Existem diversos tipos de metodologias, entre os quais:

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

Na metodologia de investigação qualitativa existem quatro categorias de tipos de estudo: exploratórios, explanatórios, descritivos e preditivos.

Sousa & Baptista (2011, p. 58) referem ainda que as abordagens qualitativas são adequadas a estudos de natureza exploratória, sendo que o estudo de caso se enquadra nesses tipos de estudo.

Assim a metodologia de pesquisa adotada assentou na recolha de dados, que serviu de base para responder às questões previamente elaboradas, considerando a proposta de um estudo de caso com propósito exploratório.

Para o efeito elaborou-se um inquérito que tem como objetivo prover dados para a análise de impacto de negócio e apoiar na escolha da melhor solução de recuperação de desastre.

3.1 ESTRATÉGIA DE PESQUISA

3.1.1 PESQUISA EXPLORATÓRIA

Segundo António Carlos Gil (2008) pode-se definir pesquisa como "… um processo formal e sistemático de desenvolvimento do método científico…", cujo propósito é identificar respostas para problemas através de metodologias científicas.

[61] São as funções, ou atividades, do negócio mais relevantes para que os objetivos e metas do negócio sejam atingidos, para que seus bens tangíveis e intangíveis sejam preservados, e para que a organização se mantenha de acordo com as leis e regulamentações que a ela se apliquem.

A pesquisa exploratória é um procedimento metodológico de abordagem qualitativa e contextual.

Piovesan & Temporini (1995) definem pesquisa exploratória como um estudo inicial que se realiza com o propósito de melhor selecionar o instrumento de medida à realidade a estudar.

No entanto, a definição comum surge dos autores Theodorson & Theodorson (1970) que referem que é estudo preliminar cujo objetivo principal é familiarizar-se com o fenómeno que está a investigar, para que o estudo, a seguir, possa ser projetado com uma maior compreensão e precisão. O estudo exploratório permite ao investigador definir uma ou mais questões e formular uma ou mais hipóteses com mais precisão. Este estudo também permite escolher as técnicas mais adequadas para as pesquisas e decidir sobre as questões, podendo alertar o investigador para as potenciais dificuldades, sensibilidades e áreas de resistência[62].

Este tipo de pesquisa adequa-se a situações em que não existe conhecimento da matéria em estudo e pode-se realizar por meio de levantamento bibliográfico, entrevistas, questionários e estudos de caso (Gil, 2008).

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

Os autores Linda Reis (2008) e António Carlos Gil (2008) referem que no caso de pesquisas que tenham como objetivo a elaboração de um trabalho académico[63] é adequado utilizar a pesquisa exploratória, considerando que esta pesquisa permite ao investigador ter uma melhor familiarização com o tema e objeto de estudo, facilitando a construção de questões relevantes para o estudo.

3.1.2 ESTUDO DE CASO

Em estudos cujo contexto de estudo são as organizações e as estratégias de gestão dos TI/SI é usual utilizar o método estudo de caso (Martins & Belfo, 2010).

Segundo os mesmos autores a sua utilização na investigação em TI/SI passa fundamentalmente por três razões: utilizar o ambiente da organização para investigar,

[62] Tradução feita a partir de 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)
[63] Dissertação, monografia

entender a natureza e complexidade dos processos em estudo e por ser um método apropriado numa área temática com poucos trabalhos conhecidos.

Estudo de caso pode ser definido como a pesquisa de um único tema, num determinado tempo e atividade, sobre a qual o investigador recolhe informação de forma detalhada, constituindo assim um estudo único e especifico sobre determinada Organização (Sousa & Baptista, 2011, p. 64).

Linda Reis (2008) define estudo de caso como sendo "…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 aspectos…".

A Tabela 13 permite sintetizar as principais características do método de estudo de caso, dando assim uma perspetiva generalista dos aspetos positivos e negativos da utilização desta metodologia.

Tabela 13 - Características principais do método estudo de caso[64]

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.

[64] Martins & Belfo, 2010, p. 45

Conforme contexto anterior esta metodologia adapta-se ao objetivo pretendido para este estudo considerando que existe a necessidade de identificar o impacto do contexto organizacional e do seu ambiente, recorrendo ao conhecimento dos conceitos para as pessoas.

Para que o resultado do estudo de caso seja válido é essencial garantir a colaboração de toda organização com o intuito de promover um melhor conhecimento da organização e de forma a contribuir para a criação de conhecimento dentro da mesma.

3.2 INSTRUMENTOS DE PESQUISA

Como instrumento de pesquisa utilizou-se um questionário semelhante ao questionário em anexo neste estudo. O questionário que permitiu recolher os dados foi elaborado por uma entidade externa com a participação da investigadora, cuja função foi fazer o levantamento que permitiu elaborar o relatório de análise de impacto negócio (análise BIA).

3.2.1 APLICAÇÃO DOS INSTRUMENTOS

Foram utilizados os dados recolhidos pelo questionário para posteriormente se escolher a melhor solução tecnológica de recuperação de desastres.

3.3 ANÁLISE DOS DADOS

Entende-se por método de análise de dados a forma como se organizam os dados recolhidos e as relações estabelecidas entre as variáveis escolhidas e as questões para as quais se pretende obter respostas (Tribunal de Contas da União, 2000).

O método utilizado neste estudo foi o questionário.

Questionário é um instrumento de investigação que tem como objetivo recolher informações com base numa amostra[65]. Para o feito são colocadas várias questões relacionadas com o tema em estudo, sem que haja interação com os inquiridos.

Existem três tipos de questionários (Sousa & Baptista, 2011): aberto, fechado e misto. O questionário aberto permite que o inquirido tenha maior liberdade nas respostas, sendo a mesma redigida pelo próprio. O questionário fechado tem por base questões de respostas fechadas o que permite comparar com outros instrumentos de recolha de informação. Os questionários mistos utilizam tanto questões que permitem respostas abertas como fechadas.

No presente estudo foram utilizados maioritariamente questionários de tipo fechado simplificando a resposta pelos inquiridos considerando que o inquirido apenas tem de optar

[65] Grupo representativo da população em estudo (Sousa & Baptista, 2011)

pela opção de resposta que mais se adequa à sua ideia e respostas de tipo aberto em respostas cujo objetivo é caracterizar determinada situação.

Os dados retirados do questionário encontram-se no capítulo 4 e, as respetivas conclusões provenientes da análise dos dados encontram-se no último capítulo desta dissertação.

4 ESTUDO DE CASO

O objetivo deste Capítulo é definir a estrutura e desenho do Estudo de Caso e justificar porque se escolheu o Estudo de Caso como método de investigação.

A recolha de dados foi privilegiada considerando que o investigador pertence à organização, tendo obtido autorização prévia do CD do Instituto Público para utilizar os dados recolhidos no decorrer da realização do projeto e atividades que lhe estão afetos.

4.1 CARACTERIZAÇÃO DO INSTITUTO PÚBLICO

O Instituto resulta da fusão de 9 organismos e é um projeto virado para a sociedade centrada na qualidade do serviço que presta às comunidades que serve.

O Instituto X conta com mais de 800 colaboradores (as) e inclui administrações descentralizadas em 5 regiões distintas.

O Instituto X, é dirigido por um CD, constituído por um presidente, um vice-presidente e dois vogais.

4.2 CARACTERIZAÇÃO DO NEGÓCIO

As suas competências são vastas, mas a sua missão é clara e focada na gestão integrada das políticas ambientais, de forma articulada com outras políticas sectoriais e tendo em vista um elevado nível de proteção e de valorização do ambiente.

A missão do Instituto é propor, desenvolver e acompanhar a gestão integrada e participada das políticas de ambiente e de desenvolvimento sustentável, de forma articulada com outras políticas sectoriais e em colaboração com entidades públicas e privadas que concorram para o mesmo fim, tendo em vista um elevado nível de proteção e de valorização do ambiente e a prestação de serviços de elevada qualidade aos cidadãos.

O Instituto pretende contribuir para o desenvolvimento sustentável de Portugal, assente em elevados padrões de proteção e valorização dos sistemas ambientais e de abordagens integradas das políticas públicas.

4.3 GESTÃO DO NEGÓCIO

4.3.1 SITUAÇÃO ATUAL

Através do levantamento de Infraestrutura e Serviços de T.I. e Comunicações foi possível identificar a situação atual da organização em estudo e retirar algumas conclusões no âmbito das tecnologias/sistemas de informação e comunicação.

O levantamento foi realizado através de questionário por uma entidade externa à organização e foi distribuído e analisado durante o mês de março de 2012 pela mesma empresa.

Para cada uma das entidades que compõem a organização os resultados encontram-se agregados da seguinte forma:

- *«Hardware»:*
  - Equipamento:
    - Servidores
    - Armazenamento
    - *«Backup»*
    - Rede
  - Sala de sistemas:
    - Condições físicas
    - Energia
    - Equipamentos
- *«Software»*:
  - Servidores
  - Postos de trabalho
- Virtualização
- Aplicações:
  - Posto de trabalho
  - Negócio
  - Correio eletrónico
- Comunicações:
  - *«WAN»*
  - Internet
  - Segurança

- Acesso remoto

- Recursos humanos

Os dados encontram-se apresentados de forma agregada no quadro abaixo:

Tabela 14 - "As Is" no âmbito das tecnologias/sistemas de informação e comunicação

"As Is" no âmbito das tecnologias/sistemas de informação e comunicação	
«Hardware»	• Muitos servidores obsoletos e sem contratos de manutenção • Parque de servidores não é uniforme relativamente a marcas ou tipo de equipamentos («*blades*», Servidores tipo «*rack*» e «*towers*») • Armazenamento não é uniforme relativamente a marcas e modelos • Equipamento de «*backup*» não uniformizado e com tecnologias obsoletas e/ou inadequadas • Postos de trabalho razoavelmente atualizados mas de características muito distintas • Parque de impressão não é uniforme
«Software»	• Múltiplos sistemas operativos, embora a maioria sejam versões de «Microsoft Windows Server» • Alguns servidores com Versões de «MS Windows Server» já obsoletas • Não existe uniformidade relativamente a Bases de Dados, embora a maioria seja «Oracle» e «MS SQL Server» • Não existe uniformidade no que diz respeito a serviço de correio eletrónico • Não existe uma imagem uniforme para os postos de trabalho, o que se traduz em múltiplas aplicações com a mesma finalidade • Múltiplas versões de «Microsoft Office», sendo algumas já obsoletas • Adoção de produtos «office open source» em 2 dos organismos não é consensual nem adotada pela totalidade dos utilizadores
Comunicação	• Soluções heterogéneas • Insuficiência de débitos Internet em algumas entidades • Contratos de comunicações já estabelecidos • Locais passíveis de descontinuação • Situações envolvendo entidades terceiras

Relativamente à situação atual do Instituto no âmbito da recuperação de desastres verificou-se que não tem implementado nenhum mecanismo de recuperação de desastres, o que significa que atualmente nenhuma das Aplicações ou Sistemas do Instituto está salvaguardado contra um desastre que afete a integridade física do edifício, danificando o centro de computação.

Verificou-se igualmente que a maioria dos servidores já se encontra numa plataforma de virtualização que tem como principais objetivos: garantir a disponibilidade de sistemas críticos para a APA, otimizar a utilização de cada servidor e simplificar a gestão e implementação de servidores. Estes objetivos são alcançados beneficiando da arquitetura «*Blade System*» existente, e com os serviços da plataforma de virtualização «*VMWare vShere*»

Atualmente existem já alguns sistemas virtualizados, no entanto, não beneficiam ainda de serviços de disponibilidade e distribuição de recursos.

Os servidores do ambiente do principal sistema de informação, baseiam-se na arquitetura «*HP Bladesystem Enclosure*» e «*Storage Externo EVA 4400*» com as seguintes características:

- *Enclosure* C7000 totalmente redundante
- *Blades* BL460 G1
- *Storage* EVA 4400 com dupla controladora FC a 4Gb

Os servidores a proteger são os seguintes:

Tabela 15 - Listagem de servidores

	Ambiente	# CPU	RAM	Disco (GB)
Ambiente de produção do principal sistema de informação				
Base de Dados	BL460	8	24	75 + 350
«*front-end*»	BL460	4	4	50 + 100
«*front-end*»	BL460	4	10	50 + 100
Correio Eletrónico				
Servidor de correio eletrónico	BL460	4	8	50 + 500
«Active Directory»				
Controlador de domínio, Serviço de resolução de Nomes (DNS), Protocolo de configuração dinâmica de anfitrião (DHCP), servidor de ficheiros	BL460	4	4	50 + 1000

4.4 VALORAÇÃO ECONÓMICA

A Tabela 16 - Elementos para valoração económica, apresenta os valores para os elementos constituintes das soluções encontradas. Os valores foram propostos pelos Fabricantes, com base num pedido de informação com o dimensionamento pretendido.

Tabela 16 - Elementos para valoração económica

Valores por item (€, sem IVA incluído)	«*Capex*»	«*Opex*»	TCO 3anos
Ligação 100Mb	9 000	1 000	45 000
Ligação 1Gb	9 000	1 400	59 400
Internet 100MBps para transferência de dados		900	32 400
Eva para replicação	102 800	0	102 800
C3000+5BL	40 000		40 000
5 DL380	25 000		25 000
3 DL380	15 000		15 000
MSA com 3TB	8 500		8 500
Co-location@Datacenter (C3K+EVA)	3 000	1 450	55 200
Co-location@Datacenter (DL380+MSA)	3 000	750	30 000
Site B OMG (C3K+EVA)	0	650	23 400
Site B OMG (DL380+MSA)	0	450	16 200
Veeam Backup[66]	4 200		4 200
Double-take[67]	25 000		25 000
Symantec Storage Foundation (Mirror Site)[68]	33 000		33 000
Symantec System Restore (Backup Site)[69]	15 000		15 000
Riverbed Appliances 5010[70]	19500		19 500
VMware® vCenter™ Site Recovery Manager™	24000		24 000
Vmware para mais 2 nós + 1 Virtualcenter	18500		18 500
Cloud			
Double-take Cloud		300	10 800
AWD 3TB + 5 servers		950	34 200

[66] Fornece proteção de dados para aplicações e dados virtualizados em «*VMware vSphere*»
[67] «*Software*» que reduz o tempo de inatividade e protege os dados para sistemas críticos em ambientes de servidor da Microsoft, em «*Red Hat Linux*» e «*VMware ESX*»
[68]Maximiza a eficiência de armazenamento, disponibilidade e desempenho através de tecnologias de virtualização, sistemas operacionais e «*hardware*» de armazenamento para construir nuvens privadas resilientes.
[69] Proporciona «*backup*» e recuperação de desastres possibilitando que as empresas recuperem do tempo de inatividade ou desastres em pouco tempo.
[70] Tecnologia que permite melhorar o desempenho de redes e aplicações em rede.

4.5 PROJETO DE RECUPERAÇÃO DE DESASTRES[71]

O objetivo principal é indicar um conjunto de cenários que permitam suportar a decisão do investimento numa solução de «*Disaster Recovery*» para o Instituto, de forma a conseguir:

- Eliminar ou minimizar responsabilidades legais, por perda de dados ou incumprimento operacional;
- Eliminar ou minimizar exposição pública negativa e problemas de reputação;
- Eliminar ou minimizar as interrupções das Operações, maximizando resiliência organizacional;
- Minimizar as necessidades de decisão durante um desastre;
- Providenciar uma recuperação ordeira e planeada;
- Minimizar potencial de perda económica.

Para obter os objetivos acima foram definidas dois parâmetros de comparação entre os cenários descritos no capítulo 4.6 Cenários:

Mirror Site[72]: RTO < 1h e RPO = 0 horas

Backup[73] Site: RTO < 8h e RPO < 24 horas

RTO - Objetivo de tempo de recuperação ou acrónimo do inglês «*Recovery time objective*»

RPO - Objetivo de ponto de recuperação ou acrónimo do inglês «R*ecovery point objective*»

[71] Ou do acrónimo inglês «*Disaster Recovery*»

[72]Espelho ou acrónimo do inglês «*mirror*» significa cópia exata de um «*site*»

[73]É a cópia de dados de um dispositivo de armazenamento a outro (CD-ROM, DVD, disco rígido, disco rígido externo (compatíveis com USB), fitas magnéticas e a cópia de segurança externa (online) para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver desaparecimentos acidentais ou corrupção de dados.

Este projeto engloba as seguintes fases:

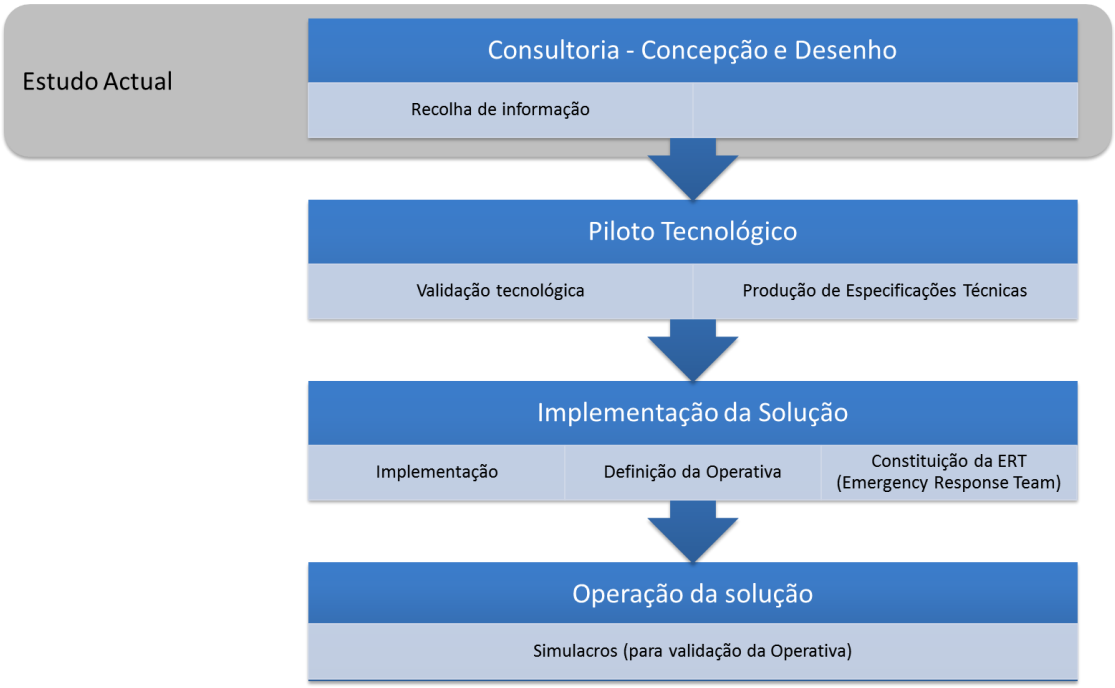


Figura 16 - Perspetiva do Estudo no contexto do Projeto Global de «*Disaster Recovery*»

4.6 CENÁRIOS

Por opção considerámos que o fornecedor do Site Secundário assegura: partilha de localização para os servidores e armazenamento, toda a solução de rede de dados, incluindo o «*core switching*»[74], o concentrador VPN para os utilizadores, o balanceamento de carga para serviços de internet, e os «*Firewalls*» para a Internet. Neste pressuposto, excluiu-se da análise de cada uma das soluções a componente de rede.

As considerações de cada cenário foram colocadas em anexo uma vez que não se pretende detalhar a solução técnica em si mas sim proceder à análise das diversas soluções em termos de «*Opex*» e «*Capex*».

[74] Geralmente as redes são construídas usando uma hierarquia de 3 camadas: núcleo, distribuição e acesso. Os «*switches*» de acesso são onde usualmente de ligam impressoras, postos de trabalho. A distribuição de interruptores é usada para agregar vários «*switches*» de acesso, etc. Os «*switches*» centrais são utilizados para transmitir quadros de dados tão rapidamente quanto possível. Os «*switches*» de core também podem ser projetados usando os protocolos L2 e L3, e o núcleo é projetado para ser tão falha tolerante e altamente disponível e tão rápida quanto possível.

4.6.1 PROJEÇÕES ECONÓMICAS

Tabela 17 - Projeções económicas para as soluções em euros

Custo 3 anos (€, sem IVA incluído)	A	B	C	E	F	G
Recovery Manager	0	33 000	15 000	42 500	22 700	10 800
Servidores Site B	40 000	25 000	25 000	15 000	15 000	0
Storage Site B	102 800	8 500	8 500	102 800	8 500	34 200
Co-location & OMG	78 600	46 200	46 200	78 600	46 200	0
Comunicações	59 400	59 400	59 400	59 400	59 400	32 400
	280 800	**172 100**	**154 100**	**298 300**	**151 800**	**77 400**
Setup (15%)	42 120	25 815	23 115	44 745	22 770	11 610
	322 920	**197 915**	**177 215**	**343 045**	**174 570**	**89 010**

4.6.2 MAPA COMPARATIVO DE CENÁRIOS

Tabela 18 - Mapa comparativo de cenários de recuperação de desastres

Cenários	Custo 3y (€, sem IVA)	RTO (h)	RPO (h)
A: Replicação F-F	322 920	0	0
B: Geocluster F-F	197 915	1	1
C: Failover F-F	177 215	8	24
E: Geocluster V-V	343 045	0	0
F: Failover V-V	174 570	4	24
G: Failover F-Cloud	89 010	2	8

5 ANÁLISE E INTERPRETAÇÃO DE DADOS E RECOMENDAÇÕES DERIVADAS DO MODELO

No que respeita ao estudo empírico concluiu-se que para que a Gestão de Topo possa tomar decisões devidamente suportadas quanto ao nível de controlo que deve estabelecer, precisa de ter confiança na análise de impacto realizada para que os custos com a gestão do negócio sejam os estritamente necessários.

Com o evoluir das novas tecnologias e com a proliferação de aplicações existentes têm-se verificado um crescimento de forma exponencial do parque informático e algumas dificuldades em acompanhar esse mesmo crescimento.

Toda a informação tem a sua segurança apenas assente em suporte magnético guardado nas instalações de cada entidade que compõe o Instituto em estudo.

Com o aumento da informação e dos problemas relacionados com o armazenamento da informação começou a ser necessário ponderar medidas alternativas para garantir a integridade dos dados.

Assim surgiram algumas perguntas críticas: quais os processos de negócio extremamente críticos e estratégicos para a organização? Qual a solução tecnológica com menor custo e que se ajusta aos parâmetros definidos nos objetivos específicos?

Houve a necessidade de internamente analisar: todas as aplicações existentes e identificar quais as mais críticas, as necessidades da infraestrutura, as necessidades das infraestruturas físicas para a criação de um centro de «*Disaster Recovery*» e quais as melhores opções do ponto de vista técnico e orçamental para a criação do mesmo.

A identificação das aplicações críticas revelou-se um trabalho complicado considerando que não foi possível aplicar o questionário de análise de impacto de negócio em anexo (Anexo 1).

De forma a dar resposta à primeira questão "Quais os processos de negócio extremamente críticos e estratégicos para a organização?" foi necessário recorrer ao estudo realizado através de consultadoria externa, cujos resultados foram aferidos com base na metodologia BIA.

Pela análise das conclusões desse estudo aferiu-se que os sistemas considerados críticos e estratégicos para o Instituto são: sistema de correio eletrónico, LDAP, arquivo de ficheiros e no principal sistema de informação, ficando assim respondida a primeira questão deste estudo.

Considerando a identificação dos sistemas críticos indicada anteriormente solicitou-se a vários fabricantes que indicassem valores, com base num pedido de informação com o dimensionamento pretendido.

Com base nos valores dados assumiu-se que o fornecedor do Site Secundário assegura: partilha de localização para os servidores e armazenamento, toda a solução de rede de dados, incluindo o «*core switching*», o concentrador VPN para os utilizadores, o balanceamento de carga para serviços de internet, e os «*Firewalls*» para a Internet. Neste pressuposto, excluiu-se da análise de cada uma das soluções a componente de rede.

Finalmente, o estudo de caso permitiu dar resposta à questão "Qual a solução tecnológica com menor custo e que se ajusta aos parâmetros definidos nos objetivos específicos?", com base na valoração económica, no estudo da situação atual da infraestrutura e considerando a definição dos seguintes parâmetros: «*Mirror Site*» com RTO < 1h e RPO = 0 horas e o «*Backup Site*» com RTO < 8h e RPO < 24 horas, foram apresentados cinco cenários possíveis cuja projeção económica e mapa comparativo se encontram descritos no subcapítulo 4.6.1 e 4.6.2, respetivamente.

No que concerne à escolha do cenário, e considerando os parâmetros definidos, face às várias opções indicadas, considerou-se que o Cenário D estaria à partida excluído pela morosidade e risco de falha do processo de gestão da configuração.

A opção que melhor se adapta à situação atual da infraestrutura é o Cenário B uma vez que cumpre objetivos mais exigentes de RPO e RTO, com um custo global apenas 12% acima das soluções de «*Failover*».

No entanto, considera-se que Cenário G também deve ser considerado pelo bom desempenho na relação custo/objetivos. No entanto, apresenta os seguintes aspetos limitativos:

- Condicionantes legais: já que os dados estarão fora do território Nacional, numa rede pública
- Segurança: As redes públicas dão menos garantias da proteção de dados.
- Maturidade Tecnológica: Estas tecnologias são emergentes.

Para concluir e, em termos do IT este projeto irá trazer inúmeras vantagens para a empresa, pois permitirá ter um projeto de recuperação de desastres para toda a estrutura existente, atualizar e otimizar a infraestrutura virtual permitindo que esta se torne mais modular ao mesmo tempo que permite consolidar a informação, reduzir custos e garantir a continuidade de negócio.

6 PERSPETIVAS DE TRABALHO FUTURO

Após a realização desta dissertação verifica-se que ainda existem algumas oportunidades de continuação e desenvolvimento deste estudo, sendo apresentado de seguida alguns tópicos suscetíveis de uma investigação mais elaborada em futuros trabalhos.

Verificar a viabilidade técnica e económica das soluções através do piloto tecnológico, considerando que se encontra terminada a fase da recolha da informação[75], sendo que a próxima fase seria a fase do piloto em que se testaria as soluções recomendadas. A planificação e custos para esta fase encontram-se descritos no Anexo 4 - Piloto Tecnológico. Quando, e se, for aceite a proposta deverá ser planeada a aquisição de serviços, tornando-se necessário reanalisar as propostas, proceder ao lançamento do concurso de aquisição da solução, seleccionar o prestador de serviço e realizar o piloto de forma a validar qual a solução que deverá ser implementada.

Proceder à avaliação da evolução tecnológica da Cloud Computing enquanto novo paradigma de solução de «*Disaster Recovery*».

Posteriormente analisar a viabilidade técnica e económica para a elaboração de um plano de continuidade de negócio.

[75] Figura 17 - Perspetiva do Estudo no contexto do Projeto Global de «Disaster Recovery»

BIBLIOGRAFIA

Abreu, J. P. (22 de agosto de 2008). Gestão do Risco nas Organizações - Continuidade de Negócio - José Pedro Abreu . Obtido em 12 de Março de 2012, de Main Road | Portal da Qualidade da Região Autónoma da Madeira: http://www.qualidademadeira.com.pt/ficheiros/documentos/Seminarios/MainRoadJoseAbreu.pdf

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 2012, de Ebook Search & Free Ebook Downloads - Ebookbrowse.com: http://ebookbrowse.com/allocate-software-bia-template-july-2011-doc-d226810122

Alves, S. (abril de 2009). ANÁLISE Critérios e Parametros para Realização do Bia - Business Impact Analysis - no PCN. GESTÃO de RISCOS, p. 48. Obtido em 9 de março de 2012, de Blog da Brasiliano & Associados: www.brasiliano.com.br

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.

Anónimo. (s.d.). Obtido em 23 de fevereiro de 2012, de www.oregon.gov: www.oregon.gov/DAS/CIO/bcp/docs/sos_bia_questionnaire.doc

Anónimo. (dezembro de 2001). Obtido em 23 de fevereiro de 2012, de www.auditnet.org: http://www.auditnet.org-/docs./BIAQuestionnaire.doc

Anónimo. (2012). Anónimo. Obtido em 05 de 06 de 2012, de Anónimo: Anónimo

Australian National Audit Office (ANAO). (2012). checklist Implementation of a business continuity management ... Obtido em 23 de fevereiro de 2012, 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 2011, de Banco de Portugal Eurosistema: http://www.bportugal.pt/pt-PT/Supervisao/ConsultasPublicas/Paginas/RelatorioconsultapublicaCNSF1_2010.aspx

Brasiliano, A. C. (março de 2009). Método avançado de análise de risco. Obtido em 19 de agosto de 2012, de Blog da Brasiliano & Associados: http://www.brasiliano.com.br/pdf/metodo_avancado_de_analise_de_riscos.pdf

British Standards Institution (BSI). (2010). BCM | Business continuity | BS25999. Obtido em 23 de Junho de 2011, de British Standards Institution: http://www.bsigroup.co.uk/en/Assessment-and-Certification-services/Management-systems/Standards-and-Schemes/BS-25999/

British Standards Institution (BSI). (2011). BS 25999 Continuidade dos Negócios. Obtido em 23 de Junho de 2011, 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 2012, de BS ISO 31100: http://www.talkingbusinesscontinuity.com/bcm-news-and-events/news/bs-311002011-risk-management-code-of-practice-and-guidance-for-the-implementation-of-bs-iso-31000-.aspx

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

California Emergency Management Agency. (6 de Junho de 2011). DISCUSSION PAPER Topic: Business Impact Analysis/Assessments. Obtido em 23 de Fevereiro de 2012, 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 2012, 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 Abril de 2012, 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 2012, 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 2012, de MediaTec Publishing Inc: http://clomedia.com/articles/view/measuring_business_results_using_business_impact_analysis

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

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

Comunidade ISMS Portugal. (2007). Comunidade Portuguesa de Segurança da Informação. Obtido em 03 de 07 de 2011, 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 2012, de Business Continuity Management Programs and Disaster Recovery Solutions: http://www.continuitysa.co.za/

Contra-Almirante Mário Carmo Durão, S.-G. A. (8 de março de 2012). Seminário "Segurança e Gestão do Risco – IESM, 08MAR12. Obtido em 19 de agosto de 2012, de AFCEA Portugal: http://www.afceaportugal.pt/2012/eventos/Apresentacao_MDN_CAlmDurao.pdf

Disaster Recovery Journal. (2012). Business Continuity Glossary by DRJ. Obtido em 27 de Agosto de 2012, de Disaster Recovery Journal: https://www.drj.com/tools/tools/glossary-2.html

Estall, H. (6 de outubro de 2010). BSI Shop - Buy British Standards. Obtido em 23 de fevereiro de 2012, 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 2012, 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 negocio. Obtido em 23 de Fevereiro de 2012, 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 09 de 2012, de SISTESEG COLOMBIA: http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

Flick, U. (2005). Métodos Qualitativos na Investigação Científica (1 ed.). (A. M. Parreira, Trad.) Monitor - projectos e edições, Lda.

Freitas, E. A. (2009). Obtido em 10 de Abril de 2012, de Biblioteca Digital da Câmara dos Deputados: http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/3564/gestao_riscos_freitas.pdf?sequence=4

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 2012, 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.

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 028 de 2012, 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 2012, de Official Blog for Dr Goh Moh Heng: http://www.goh-moh-heng.com/2011/07/26/bcm-concept-rto-rpo-mtpd/defining-rto/

Human Code. (2010). Relatório de Progresso Estudo de Disaster Recovery. Lisboa.

Information Security Office. (s.d.). Obtido em 7 de fevereiro de 2012, de Information Security Office: http://security.utexas.edu/risk/planning/UT-Austin-BIA-Template.doc

Infosistema. (2010). Infosistema » Plano Continuidade Negócio. Obtido em 03 de 07 de 2011, de Consultoria de TI: http://www.infosistema.pt/consultoria-de-ti/plano-de-continuidade-de-negocio/

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/iso-27005.htm

Kirvan, P. (julho de 2009). Using a business impact analysis (BIA) template: A free BIA template and guide. Obtido em 8 de fevereiro de 2012, de http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-analysis-BIA-template-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 2011, de Handbook of Information Security Management: http://www.blacksheepnetworks.com/security/info/misc/handbook/223-228.html

Leonarde, A. (s.d.). Obtido em 10 de setembro de 2012, de Prof. Alexandre Leonarde: http://www.leonarde.pro.br/classificacaodaspesquisas.pdf

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

Maria Manuela Gaivéo, C. n. (2007). BS 25999: Código de Práticas para a Gestão da Continuidade do Negócio. Obtido em 03 de 07 de 2011, de Comunidade ISMS Portugal: http://ismspt.blogspot.com/2006/11/continuidade-de-negcio.html

MarkH927@aol.com. (19 de março de 2001). Obtido em 8 de fevereiro de 2012, 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.

MENEZES, L. C. (2009). GESTÃO DE PROJETOS (3ª ed.). Atlas. Obtido em 10 de 04 de 2012, de http://www.tenstep.com.br/br/Newsletter/AImportanciadoGerenciamentodeRisco.htm

Moreira, L. O., Monteiro, M. A., & Pinto, Y. M. (2009). Análise comparativa de riscos em segurança de informação de um ERP de uma indústria farmacêutica. Rio de Janeiro.

Mrasmussen. (24 de Novembro de 2009). Good Risk Management Guidance – Here At Last in ISO 31000 Corporate Integrity. Obtido em 03 de 06 de 2012, de Corporate Integrity, LLC: http://www.corp-integrity.com/risk-management/good-risk-management-guidance-here-at-last-in-iso-31000

NACIONAL, M. D. (2000). Disaster info desastres. Obtido em 13 de Agosto de 2012, de DISASTER info DESASTRES - Partners / PAHO: http://www.disaster-info.net/PED-Sudamerica/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 2012, 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 2012, 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 2012, de Business Resumption Planners Association: http://www.brpa-chicago.org/docs/BRPA%20-%20BIA%20Presentation%20(BP).pdf

Peltier, T. R. (2001). Information Security Risk Analysis. AUERBACH publications. Obtido em 7 de fevereiro de 2012, de The Institute of Internal Auditors: www.theiia.org/download.cfm?file=63258

Piovesan, A., & Temporini, E. R. (29 de Abril de 1995). Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública. Revista Saúde Pública, pp. 318-325.

Portal, T. I. (2008). Introduction to ISO 27005 - ISO27005. Obtido em 3 de junho de 2012, 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.

Rochester Institute of Technology. (agosto de 2008). Obtido em 23 de fevereiro de 20121, de Rochester Institute of Technology: http://www.rit.edu/fa/buscont/sites/rit.edu.fa.buscont/files/docs/bia_template_rit.doc

Rosa, C. A. (2009). Como elaborar um plano de negócio. Como elaborar um plano de negócio. (S. B. Sebrae, Ed.) Brasilia, Brasilia.

Semana Informática. (20 a 26 de Maio de 2011). Semana Informática. Continuidade do negócio é fucral(Informática), 1023, 35. Semana Informática.

Serrano, A., & Jardim, N. (2007). Disaster recovery : um paradigma na gestão do conhecimento /. Lisboa: FCA - Editora de Informática.

Silberman, T. D., & Mattos, U. A. (janeiro a abril de 2008). METODOLOGIA PARA ANÁLISE DE RISCO: ESTUDO EM UMA UNIDADE DE CO-GERAÇÃO DE ENERGIA DE UM SHOPPING CENTER DE MACAÉ. Boletim Técnico Organização & Estratégia, 4, pp. 155-172.

Silva, A. L. (2003). Departamento de Computação. Obtido em 12 de Março de 2012, de Universidade Estadual de Londrina: http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&sqi=2&ved=0CCgQFjAB&url=http%3A%2F%2Fwww2.dc.uel.br%2Fnourau%2Fdocument%2F%3Fview%3D195&ei=L7Y7UKLdOOmM0AW444HADg&usg=AFQjCNFHyl7AU6eA58bRzlSHxnY80ijZrQ&sig2=mF48G8C6YydID6VFcoJ93

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 2011, 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 2012, de Purdue University: http://www.purdue.edu/securepurdue/docs/training/BusinessContinuityPlanning.ppt

Sonaecom. (2009). Sonaecom: Annual Report 2009. Obtido em 03 de 07 de 2011, 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 Politica Contemporânea.

Stoneburner, G., Goguen, A., & Feringa, A. (Julho de 2002). National Institute of Standards and Technology. Obtido em 3 de Outubro de 2012, de NIST.gov - Computer Security Division - Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-30/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.

Theodorson, G. A., & Theodorson, A. G. (1970). Modern dictionary of sociology. Londres.

Tribunal de Contas da União. (2000). Manual de Auditoria da Natureza Operacional. Brasília: Divisão de Documentação do TCU.

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.

Turnbull, M. (14 de Novembro de 2011). Obtido em 23 de fevereiro de 2012, 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). A Risk Management Standard.

University of Toronto Information. (2011). CSA - Disaster Recovery Planning. Obtido em 27 de Junho de 2011, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#descr

Walch, D. N. (2012). Continuity Central. Obtido em 23 de Fevereiro de 2012, de Continuity Central: http://www.continuitycentral.com/givebiatheaxe.pdf

Wikipedia. (27 de Dezembro de 2011). ISO/IEC 17799. Obtido em 14 de Agosto de 2012, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ISO/IEC_17799

Wikipedia. (12 de Fevereiro de 2012). ITILv3. Obtido em 14 de Agosto de 2012, 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 2012, 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 2012, 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 2012, 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 2012, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/Obsolesc%C3%AAncia

OBRAS CITADAS

Alves, S. (abril de 2009). ANÁLISE Critérios e Parametros para Realização do Bia - Business Impact Analysis - no PCN. *GESTÃO de RISCOS*, p. 48. Obtido em 9 de março de 2012, de Blog da Brasiliano & Associados: www.brasiliano.com.br

Brasiliano, A. C. (março de 2009). *Método avançado de análise de risco.* Obtido em 19 de agosto de 2012, de Blog da Brasiliano & Associados: http://www.brasiliano.com.br/pdf/metodo_avancado_de_analise_de_riscos.pdf

California Emergency Management Agency. (6 de Junho de 2011). *DISCUSSION PAPER Topic: Business Impact Analysis/Assessments.* Obtido em 23 de Fevereiro de 2012, de Cal E.M.A: http://www.calema.ca.gov/PlanningandPreparedness/Documents/DP BIA 081208.doc

Cavalcanti, C. D. (2009). *Gestão de Riscos - Abordagem de conceitos e aplicações.* Obtido em 10 de Abril de 2012, de Convergência Digital Blog publicado por Carlos Diego Cavalcanti Artigos e Análises: http://www.valcann.com/publicacoes/riscos_conceitosaplicacoes.pdf

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 2012, de MediaTec Publishing Inc: http://clomedia.com/articles/view/measuring_business_results_using_business_impact_analysis

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

Disaster Recovery Journal. (2012). *Business Continuity Glossary by DRJ.* Obtido em 27 de Agosto de 2012, de Disaster Recovery Journal: https://www.drj.com/tools/tools/glossary-2.html

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

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 negocio.* Obtido em 23 de Fevereiro de 2012, de SISTESEG COLOMBIA: http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.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 2012, 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.

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 028 de 2012, 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 2012, de Official Blog for Dr Goh Moh Heng: http://www.goh-moh-heng.com/2011/07/26/bcm-concept-rto-rpo-mtpd/defining-rto/

Infosistema. (2010). *Infosistema » Plano Continuidade Negócio*. Obtido em 03 de 07 de 2011, de Consultoria de TI: http://www.infosistema.pt/consultoria-de-ti/plano-de-continuidade-de-negocio/

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/iso-27005.htm

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 06 de 2012, de Corporate Integrity, LLC: http://www.corp-integrity.com/risk-management/good-risk-management-guidance-here-at-last-in-iso-31000

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 2012, de ABEPRO: http://www.abepro.org.br/biblioteca/ENEGEP2004_Enegep0802_1822.pdf

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 2012, de Business Resumption Planners Association: http://www.brpa-chicago.org/docs/BRPA%20-%20BIA%20Presentation%20(BP).pdf

Piovesan, A., & Temporini, E. R. (29 de Abril de 1995). Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública. *Revista Saúde Pública*, pp. 318-325.

Portal, T. I. (2008). *Introduction to ISO 27005 - ISO27005*. Obtido em 3 de junho de 2012, 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.

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 2011, de Sinfic SA: http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=23757

Sonaecom. (2009). *Sonaecom: Annual Report 2009*. Obtido em 03 de 07 de 2011, 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 Politica Contemporânea.

Stoneburner, G., Goguen, A., & Feringa, A. (Julho de 2002). *National Institute of Standards and Technology*. Obtido em 3 de Outubro de 2012, de NIST.gov - Computer Security Division - Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-30/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.

Tribunal de Contas da União. (2000). *Manual de Auditoria da Natureza Operacional.* Brasília: Divisão de Documentação do TCU.

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.

UK - The Institute of Risk Management; The Association of Insurance and Risk Managers; The National Forum for Risk Management. (2002). *A Risk Management Standard.*

University of Toronto Information. (2011). *CSA - Disaster Recovery Planning.* Obtido em 27 de Junho de 2011, de http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm#descr

Wikipedia. (27 de Dezembro de 2011). *ISO/IEC 17799*. Obtido em 14 de Agosto de 2012, de Wikipedia, the free encyclopedia: http://pt.wikipedia.org/wiki/ISO/IEC_17799

Wikipedia. (12 de Fevereiro de 2012). *ITILv3*. Obtido em 14 de Agosto de 2012, 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 2012, 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 2012, de Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/ISO_31000

GLOSSÁRIO

Alta disponibilidade – A capacidade de um sistema para executar as suas funções, sem interrupção por um período prolongado de tempo.

Ambiente Externo – É o levantamento de cenários prospetivos, identificando fatores externos incontroláveis, mas que influenciam na concretização de perigos. Inclui o levantamento dos índices de criminalidade, estrutura do crime organizado, mercados paralelos, estrutura do judiciário, corrupção policial, ambiência no entrono, entre outros.

Ambiente Interno – é o levantamento do nível de relacionamento dos colaboradores e Organização. Inclui desde políticas de remuneração até políticas de recursos humanos.

Ameaça – episódio ou atitude indesejável que potencialmente remove, desabilita ou arruína um recurso informático e, portanto, as informações a ele ligadas.

Análise de risco – consiste em determinar efeitos dos eventos de risco identificados e as suas probabilidades de ocorrência, tendo em conta a existência ou não de controlos e a sua eficiência.

Análise do impacto nos negócios (BIA) – A análise BIA, de forma simplificada, pode ser considerada como um processo de análise das funções do negócio e o efeito que uma disrupção no negócio poderá ter sobre as mesmas.

Ataque – corresponde à concretização de uma ameaça.

Ativação – Quando todos os procedimentos de continuidade do negócio e de recuperação de desastres foram colocados em ação.

Atividade – Processo ou conjunto de processos existentes que produzem ou suportam um ou mais produtos ou serviços, em determinada organização.

Autenticidade – garantia de que a informação é de facto proveniente da origem mencionada.

Avaliação de risco – é um processo global que inclui a identificação, análise e valorização de risco.

«Backup» – é a cópia de dados de um dispositivo de armazenamento a outro (CD-ROM, DVD, disco rígido, disco rígido externo (compatíveis com USB), fitas magnéticas e a cópia de segurança externa (online) para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver desaparecimentos acidentais ou corrupção de dados.

Defeito ou acrónimo do inglês «*bug*» – erro no funcionamento de um «*software*» ou também de «*hardware*»

Cadeia de valor – "A cadeia de valor designa uma série de atividades relacionadas e desenvolvidas pela empresa a fim de satisfazer as necessidades dos clientes…" (Moura, 2006)

CAPEX ou Despesas de capital/investimento em bens de capital ou acrónimo do inglês «*capital expenditure*» – o montante de investimentos realizados de forma a manter em funcionamento um negócio ou um determinado sistema.

«Cloud computing» – O conceito de computação em nuvem refere-se à utilização da memória e das

capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet. O armazenamento de dados é feito em serviços que poderão ser acedidos de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas x ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet – daí a alusão à nuvem.

«Cold-site» – propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações. É aplicável apenas em situações em que a tolerância de indisponibilidade é muito grande.

Confidencialidade – garantia de que os utilizadores devidamente autorizados obtenham acesso à informação e aos recursos correspondentes, sempre que necessário, isto é, garantia de que a informação apenas esta acessível a pessoas autorizadas a realizar tal acesso.

Continuidade de negócio – capacidade estratégica ou tática de uma organização em planear e responder a incidentes ou disrupções ao negócio de modo a garantir a continuidade das operações de negócio a um nível considerado aceitável**.**

«Core switching» – Geralmente as redes são construídas usando uma hierarquia de 3 camadas: núcleo, distribuição e acesso. Os «*switches*» de acesso são onde usualmente de ligam impressoras, postos de trabalho. A distribuição de interruptores é usada para agregar vários «*switches*» de acesso, etc. Os «*switches*» centrais são utilizados para transmitir quadros de dados tão rapidamente quanto possível. Os «*switches*» de «*core»* também podem ser projetados usando os protocolos L2 e L3, e o núcleo é projetado para ser tão falha tolerante e altamente disponível e tão rápida quanto possível.

Custo total da posse ou acrónimo do inglês «*Total cost of ownership*» (**TCO) –** estimativa financeira para determinado investimento.

Desastre – Qualquer interrupção, falha, evento ou problema que pode causar perdas e provocar um impacto arrasador na organização.

Disponibilidade – Um sistema que está disponível para fornecer serviços de acordo com o seu projeto, sempre que uma solicitação for realizada.

«Downtime» – Tempo de indisponibilidade de um serviço, processo ou aplicação.

E-business acrónimo do inglês «*Electronic Business*» (negócio eletrônico) – é o termo que se utiliza para identificar os negócios efetuados por meios eletrônicos, geralmente na Internet. Muitas vezes é associado ao termo comércio eletrônico. Pode-se definir e-business como negócios feitos através da Internet no sentido mais amplo da palavra negócio, desde contatos diretos com consumidores, fornecedores como também análises de mercado, análises de investimentos, busca de informações sobre o macro ambiente, pesquisa de mercados, etc.

Espelho ou acrónimo do inglês «*mirror*» – significa cópia exata de um site

Estrutura da gestão de risco – conjunto de componentes que fornecem as bases e modalidades de organização de conceção, execução, acompanhamento, revisão e melhorar continuamente a gestão

dos riscos em toda a organização.

F-Cloud – relação 1:n de servidores físicos para virtuais numa nuvem pública

F-F – relação 1:1 entre servidores físicos

«Failover» – «*site*» secundário recebe backups do site de produção, com uma determinada periodicidade (1 vez por dia, ou várias vezes por dia).

Falha – evento que ocorre e impossibilita os utilizadores de acederem aos sistemas ou aplicações.

Falha de rede – Interrupção na disponibilidade de acesso aos sistemas com origem numa falha de comunicação, que afeta: uma rede de computadores, terminais, servidores ou postos de trabalho.

«Firewall» – é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controlo da rede. A sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou receção de acessos nocivos ou não autorizados de uma rede para outra. Este conceito inclui os equipamentos de filtros de pacotes e de «*proxy*» de aplicações, comummente associados a redes TCP/IP.

«*Framework*» – Conjunto de métodos e técnicas destinadas a representar, verificar e validar determinado modelo.

«*Front-end*» – parte do sistema de «*software*» que interage diretamente com o utilizador.

Função crítica do negócio – São as funções, ou atividades, do negócio mais relevantes para que os objetivos e metas do negócio sejam atingidos, para que seus bens tangíveis e intangíveis sejam preservados, e para que a organização mantenha-se de acordo com as leis e regulamentações que a ela se apliquem.

Funções Críticas – Informação que não pode ser interrompida ou ficar indisponível por um determinado período de tempo.

«*Gigabyte*» - é uma unidade de medida de informação que equivale a 1 000 000 000 «*bytes*»

«Geocluster» – «*site*» secundário é atualizado em contínuo por um sistema de «*cluster*» (semelhante ao espelho, mas com algum atraso).

Gestão de continuidade de negócios (BCM) – É o ato de antecipar incidentes que afetarão as funções de missão críticas e processos para a organização e garantindo que ele responde a qualquer incidente, de forma planeada e ensaiada.

Gestão de risco – coordenação de atividades para dirigir e controlar o risco numa organização, isto é, processo global de identificação, análise e avaliação do risco.

«Hardware» – pode ser definido como um termo geral para equipamentos.

***«Hot-site»* –** Uma instalação de centro de dados ou instalação de escritório com *"hardware»* suficiente, interfaces de comunicação e espaço de ambiente controlado capaz de fornecer relativamente um sistema de *backup* imediato de apoio de processamento de dados.

Identificação de risco – é identificar as fontes de risco e as situações existentes, internas ou externas, que possam afetar os objetivos da organização.

Incidente – um acontecimento que envolve uma infração de segurança ou situação que pode ser, ou que se pode levar, a uma disrupção, perda, emergência ou crise no negócio.

***«Inputs»* –** Entradas de um determinado processo ou sistema.

Integridade – A propriedade de manutenção dos dados da forma como foram criadas, não sofrendo alteração durante a sua manipulação, isto é, garantia da não violação da informação e dos métodos de processamento da mesma. A integridade garante que as informações armazenadas ou transmitidas estão em conformidade, não tendo sido corrompidas, alteradas ou violadas de alguma forma.

Memória de acesso aleatório ou acrónimo do inglês «*Random Access Memory*» (RAM) – é um tipo de memória que permite a leitura e a escrita.

Não repúdio – garantia de que não se pode negar a autoria da informação, ou o caminho por ela transitado.

OPEX ou despesas operacionais ou acrónimo do inglês «*operational expenditure*» – custo associado à manutenção negócio ou sistema.

Planeamento de continuidade de negócios (BCP) – O planeamento antecipado e preparações que são necessários para identificar o impacto das perdas potenciais, para formular e implementar estratégias de recuperação viável, desenvolver plano de recuperação (s) que asseguram a continuidade dos serviços organizacionais, no caso de uma emergência ou desastre, e para administrar testes e programas de manutenção.

Plano de continuidade de negócios (PCN) – é uma metodologia elaborada para garantir a recuperação de um ambiente de produção, independentemente de ocorrências que suspendam suas operações e dos danos nos componentes («software», *«hardware»*, infraestrutura, etc.) por ele utilizados.

Plano de gestão – regime no âmbito da gestão de risco especificando a abordagem, os componentes de gestão e recursos para ser aplicado à gestão de risco.

Plano de recuperação de desastres (PRD) – Documento que define os recursos, ações, tarefas e os dados necessários na gestão do processo de recuperação dos serviços de uma organização.

Ponto de recuperação objetivo (PRO/RPO) – Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a organização determina por "perda aceitável" numa situação de desastre, isto é, representa a grandeza do volume de perda de dados em que uma organização pode incorrer na sequência de uma anomalia, sem se verificar um impacto expressivo.

O RPO permite que a organização defina uma janela de tempo, antes que um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais.

Esta métrica pode ser medida em volume de dados ou pelo tempo que decorre entre as atualizações de

dados. O que diferencia o tempo de RPO é a tecnologia que a organização utiliza para fazer a atualização dos dados.

Processo de gestão de risco – aplicação sistemática de políticas de gestão, procedimentos e práticas para as atividades de comunicação, consultoria, estabelecer o contexto e identificar, analisar, avaliar, tratar, monitoramento e revisar risco.

Processo de recuperação de dados – recuperação de dados armazenados em unidades de armazenamento danificadas, tais como, *tapes* ou discos.

Protocolo de configuração dinâmica de anfitrião ou acrónimo do inglês *«Dynamic Host Configuration Protocol»* *(DHCP)* – de forma sucinta é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços de Protocolo de internet.

***«Proxy»* –** O «*proxy*» serve como um intermediário entre os computadores de uma rede e a Internet. Um servidor «*proxy*» pode ser usado basicamente com três objetivos: partilhar a conexão da Internet quando existe apenas um protocolo de internet disponível, melhorar o desempenho do acesso através de uma cache de páginas e bloquear acesso a determinadas páginas.

Rede de área alargada ou Rede de longa distância ou acrónimo do inglês «*Wide Area Network*» (WAN) – é uma rede de computadores que abrange uma grande área geográfica.

Recuperação alternativa – Métodos selecionados para a recuperação das funções consideradas críticas para o negócio após a ocorrência de um desastre ou interrupção dos serviços críticos, definidos como «*hot-site*», «*cold-site*», «*mobile shell*» ou centro de comandos.

Recuperação de tempo objetivo (RTO) – Período a partir do qual todos os dados e serviços críticos têm de estar operacionais. Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a organização determina por "perda aceitável" em situação de desastre. O RPO permite que a organização defina uma janela de tempo, antes que um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais.

De forma simplificada pode entender-se o RTO como o período de tempo necessário para recuperar os sistemas ou aplicações.

Replicação – «*site*» secundário é um espelho em tempo real do *«site»* de produção.

Replicação aplicacional – Diretamente associado à recuperação dos serviços de *«software»* e aplicações da organização e dos respetivos dados, após os Sistemas de Informação terem sido repostos ou substituídos.

Risco – ação que causa impacto nos resultados de uma organização. O risco pode ser classificado em vários níveis, nomeadamente: baixo, médio ou alto. Para os vários níveis de risco deve-se analisar qual a importância da consequência que ele provoca na organização. Um risco de nível baixo tem pouco impacto na organização, enquanto um risco alto tem impacto muito forte.

De forma sucinta risco pode ser definido como uma perda.

Risco de gestão política – declaração das intenções gerais e direção de uma organização relacionadas com a gestão de risco.

Risco de negócio - Geralmente são relacionados a fatores externos à organização, como, por exemplo, os aspetos econômicos, competitivos, legais, etc. Este tipo de análise suporta a toma de decisões no plano estratégico da Organização.

Risco Operacional – está estreitamente relacionado com as operações internas da organização.

Segurança – é a perceção de se estar protegido de riscos, perigos ou perdas.

Sistema central de diretório ou acrónimo do inglês «*Lightweight Directory Access Protocol*» (LDAP) – é um protocolo que serve para atualizar e pesquisar diretórios sobre TCP/IP, isto, reflete estruturas que podem representar pessoas, unidades organizacionais, impressoras, documentos, grupos de pessoas, etc.

Sítio da internet ou do acrónimo do inglês «*site*» – sítio eletrónico/WWW/da internet

Sistema crítico – Um sistema crítico é um serviço de informação considerado essencial para uma função crítica do negócio

«Software» – é um programa de computador.

«Switch» – elemento ativo que age no nível 2 do modelo OSI, é um equipamento que interliga os computadores em rede.

Tempo de recuperação – Período correspondente entre a declaração de desastre ou a ativação da recuperação do desastre até á recuperação das funções críticas para o negócio.

Tempo máximo tolerável de inatividade ou acrónimo do inglês «*Maximum Tolerable Downtime*» (MTD) – Especifica o período máximo de tempo que um determinado processo empresarial pode estar inoperante antes de sobrevivência da organização está em risco.

Teia mundial ou acrónimo do inglês World Wide Web (WWW) – é um sistema de documentos em hipermédia que são interligados e executados na Internet.

Tratamento de risco – ajudar na redução do risco através do seu tratamento através da seleção de um ou mais cenários de solução.

Unidade central de processamento ou acrónimo do inglês «*Central Processing Unit*» (CPU) – é a parte de um sistema computacional, também conhecido como processador

V-V – relação n:n entre servidores virtuais

Valorização do risco – estimar o valor do dano e comparar os valores estimados do risco com critérios de risco, com a finalidade de determinar a significância do nível e tipo de risco.

Vulnerabilidade – debilidade ou insuficiência que faz com que uma determinada ameaça ocorra.

«Warm-site» – aplica-se a sistemas com maior tolerância à paralisação, podendo estar sujeita à indisponibilidade por mais tempo até ser possível retomar a operacionalidade sem, no entanto, comprometer o serviço ou gerar impactos significativos.

ÍNDICES REMISSIVOS

A

Análise de impacto de negócio, LIII
- Benefícios, LX
- Conceito, LIII
- Elementos, LVI
- Exemplos de atividades críticas, LX
- Metodologia, LVII
- Objetivos, LIX
- Variáveis
  - Dependências, LV
  - Impacto Negócio
    - Critérios, XLVI
  - Impactos Financeiros, LV
  - Impactos Operacionais, LV
  - Níveis de Impacto Negócio
    - Categorias, XLVI
  - Níveis de Tolerância, LV
  - Procedimentos alternativos, LV
  - Recuperação de tempo objetivo (RTO), LV
- Variáveis, LIV

Análise de risco, XLVII
- Guia *PMBoK*, LI
- Metodologia, XLIX
  - Análise de Processo, L
  - Análise Técnica, L
  - Conjunto Análise, L
- Normas
  - BS ISO 31100, LII
  - COBIT 5, LII
  - ISO 27002, LII
  - ISO 27005, LII
  - ISO/IEC 17799/2003, LII
  - ITIL v.3, LII
- Normas, LII
- objetivo, XLVIII
- Risco
  - Categorias, XLVIII
  - Elementos, XLVIII
  - Risco de Negócio, XLVIII
  - Risco Operacional, XLVIII

E

Estudo de caso, LXV
- Caracterização da organização, LXV
  - Caracterização do negócio, LXV
  - Gestão do negócio
    - Situação atual, LXVI
  - Gestão do negócio, LXVI

G

Gestão de risco, XXXV

Gestão de Risco
- Benefícios, XXXVIII
- Classificações de Risco, XXXVII
  - Risco de acesso, XXXVII
  - Risco de continuidade, XXXVII
  - Risco de estratégia, XXXVII
  - Risco de flexibilidade, XXXVII
  - Risco de integridade, XXXVII
- Dicionário de riscos, XXXVIII
- Etapas, XXXVI
- Normalização
  - ISO 27005, XLVII
  - ISO 31000, XLVII
- Normalização e boas práticas, XXXIX

M

Metodologia de pesquisa, LXI
- Estratégia de pesquisa
  - estudo de caso, LXIII
  - pesquisa exploratória, LXII
- Instrumentos, LXIV
  - Análise dos Dados, LXIV
  - aplicação dos instrumentos, LXIV

P

PLANO DE CONTINUIDADE DE NEGÓCIO

10 Elementos fundamentais, XXV
Análise de Impacto Estratégia, XXX
Benefícios, XXXIV
Composição, XIX
Definições e Conceitos, XX
Elementos Chave, XIX
Estratégias de recuperação, XXXII
Cold-site, XXXII
Hot-site, XXXII
Warm-site, XXXII
Gestão, XXXIII
Impacto versus probabilidade, XXI
Implementação, XXXIII
Metodologia, XXV
Plano de gestão de crise, XIX
Plano de processos alternativos de negócio, XIX
Plano de recuperação tecnológica, XIX
Plano de resposta de emergência, XIX
Ponto de Retorno Objetivo, XXII
Prejuízo versus Impacto, XXII
Segurança e Risco, XX
Tempo de Retorno Objetivo, XXII

ANEXOS

Anexo 1

Questionário de impacto de negócio

Anexo 2

Pré-Teste

Anexo 3

Cenários de estratégias de recuperação de desastre

Anexo 4

Piloto Tecnológico

Anexo 5

Considerações adicionais dos cenários

ANEXO 1 - QUESTIONÁRIO DE IMPACTO DE NEGÓCIO

QUESTIONÁRIO ANÁLISE DE IMPACTO DE NEGÓCIO

INTRODUÇÃO

O presente questionário é componente de uma pesquisa feita no âmbito do Mestrado de Gestão de Empresa da Universidade Lusófona de Humanidades e Tecnologias – Faculdade de Economia e Gestão, e foi distribuído na Organização em estudo.

O objetivo deste questionário é apoiar no desenvolvimento do Plano de Continuidade de Negócio (PCN) deste Instituto Público. Durante o processo de preparação do desenvolvimento de um PCN, é importante entender os processos de negócio e o seu impacto sobre a Organização.

Este Instituto Público é composta por diversas operações que são constituídas por inúmeras tarefas relacionadas entre si e, todos os processos de negócios são focados no fornecimento de um serviço para entidades internas ou externas.

Nem todos os processos são essenciais, no entanto, todos os processos fornecem um serviço completo de negócios. Serviços que afetam diretamente a capacidade deste Instituto Público para cumprir os seus objetivos de missão críticos que devem ser recuperados de forma mais apropriada face a um desastre. Enquanto outros serviços, apesar de importantes, não apresentam a mesma criticidade ou impacto podendo a sua recuperação ser adiada.

De forma a identificar e priorizar os processos de negócios mais críticos será solicitado o apoio dos diversos departamentos. A informação recolhida será usada para determinar, de forma global, as prioridades de negócio.
As perguntas foram desenvolvidas para elucidar sobre diversas aspetos, tais como o impacto financeiro, o tempo para recuperação e requisitos de recursos. As respostas serão compiladas e analisadas para fornecer as informações necessárias para desenvolver uma estratégia de recuperação de negócios de toda a Organização.

Por favor, preencha este questionário com tanto detalhe quanto o possível. A sua contribuição é valiosa para o desenvolvimento de um plano de continuidade de negócios eficaz.

Muito obrigado pela colaboração.

Análise de Impacto de Negócio (BIA).

A fase inicial do projeto de Plano de Continuidade de Negócios é o desenvolvimento de uma Análise de Impacto de Negócio (BIA).
Uma análise de impacto de negócios é um processo utilizado para determinar o efeito de uma interrupção de serviços em cada unidade de negócio e na Organização como um todo.

A análise BIA vai identificar funções críticas e descrever o que seria necessário para recuperar essas funções, em caso de desastre ou interrupções no serviço na medida em que providencia informação valiosa sobre os impactos de um desastre, no curto e longo prazo.

As informações recolhidas na análise BIA serão usadas para:

- Determinar a prioridade para restaurar as funções da Organização;
- Identificar recursos críticos necessários para apoiar a recuperação do negócio de cada

departamento;

- Identificar os requisitos de infraestrutura de tecnologia crítica;
- Identificar processos de negócios e priorizá-los de acordo com a criticidade.
- Identificar o objetivo de tempo de recuperação (RTO) associados a cada processo de negócio crítico;
- Identificar o objetivo de ponto de recuperação (RPO) associados a cada processo de negócio crítico;
- Identificar sistemas, equipamentos e aplicativos associados a cada processo de negócio crítico;
- Identificar os impactos quantitativos e qualitativos que advêm da ocorrência de uma interrupção ocorrer;
- Identificar interdependências críticas associadas com a unidade de negócios e seus processos.

Conceito de RPO e RTO

Ponto de recuperação objetivo (RPO)

Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a Organização determina por "perda aceitável" numa situação de desastre, isto é, representa a grandeza do volume de perda de dados em que uma Organização pode incorrer na sequência de uma anomalia, sem se verificar um impacto expressivo.
O RPO permite que a Organização defina uma janela de tempo, antes que um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais.

Esta métrica pode ser medida em volume de dados ou pelo tempo que decorre entre as atualizações de dados. O que diferencia o tempo de RPO é a tecnologia que a Organização utiliza para fazer a atualização dos dados.

Prioridade	RPO
0	No ponto de falha, o melhor cenário é que nenhum dos dados seja perdido; no entanto, é provável que apenas a última transação, antes do desastre, se perca durante a transmissão.
1	Nas últimas oito horas, independentemente de quando ocorre a interrupção no serviço.
2	Como era no início do dia útil (08:00 horas). Todos os dados inseridos desde o último backup terão de ser reconstruído no sistema.
3	A partir do *backup* realizado no sábado ou no domingo à noite, antes do desastre mais recente. Todos os dados inseridos desde o último *backup* terão de ser reconstruídos no sistema.

Tabela 1 - RPO

Recuperação de tempo objetivo (RTO)

Período a partir do qual todos os dados e serviços críticos têm de estar operacionais. Descreve a quantidade aceitável de perda de dados medidos em tempo. O objetivo do ponto de recuperação é o ponto no tempo em que se deve recuperar os dados, conforme definido pela sua organização. Geralmente é uma definição do que a Organização determina por "perda aceitável" numa situação de desastre. O RPO permite que a Organização defina uma janela de tempo, antes que um desastre, durante o qual os dados podem ser perdidos. O valor dos dados nesta janela pode ser comparado com o custo da prevenção de desastres adicionais.
De forma simplificada pode entender-se o RTO como o período de tempo necessário para recuperar os sistemas ou aplicações.

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

Tabela 2 - RTO

Estimativa do impacto qualitativo

Em primeiro lugar, é necessário identificar os impactos de interrupção de negócios intangíveis resultantes de uma interrupção do processo de negócio. Use os dados fornecidos na Tabela 3 - Estimativa do impacto qualitativo.

Estimativa do impacto qualitativo	
Pontuação	Impacto para o negócio
0 a 1 semana	Nada
1 a 2 semanas	Pouca
2 a 3 semanas	Mediana
3 semanas a 1 mês	Bastante
Superior a 1 mês	Extremamente

Tabela 3 - Estimativa do impacto qualitativo

Informação do departamento/divisão

Nome do departamento/divisão

Listagem de Processos

Listagem de processos

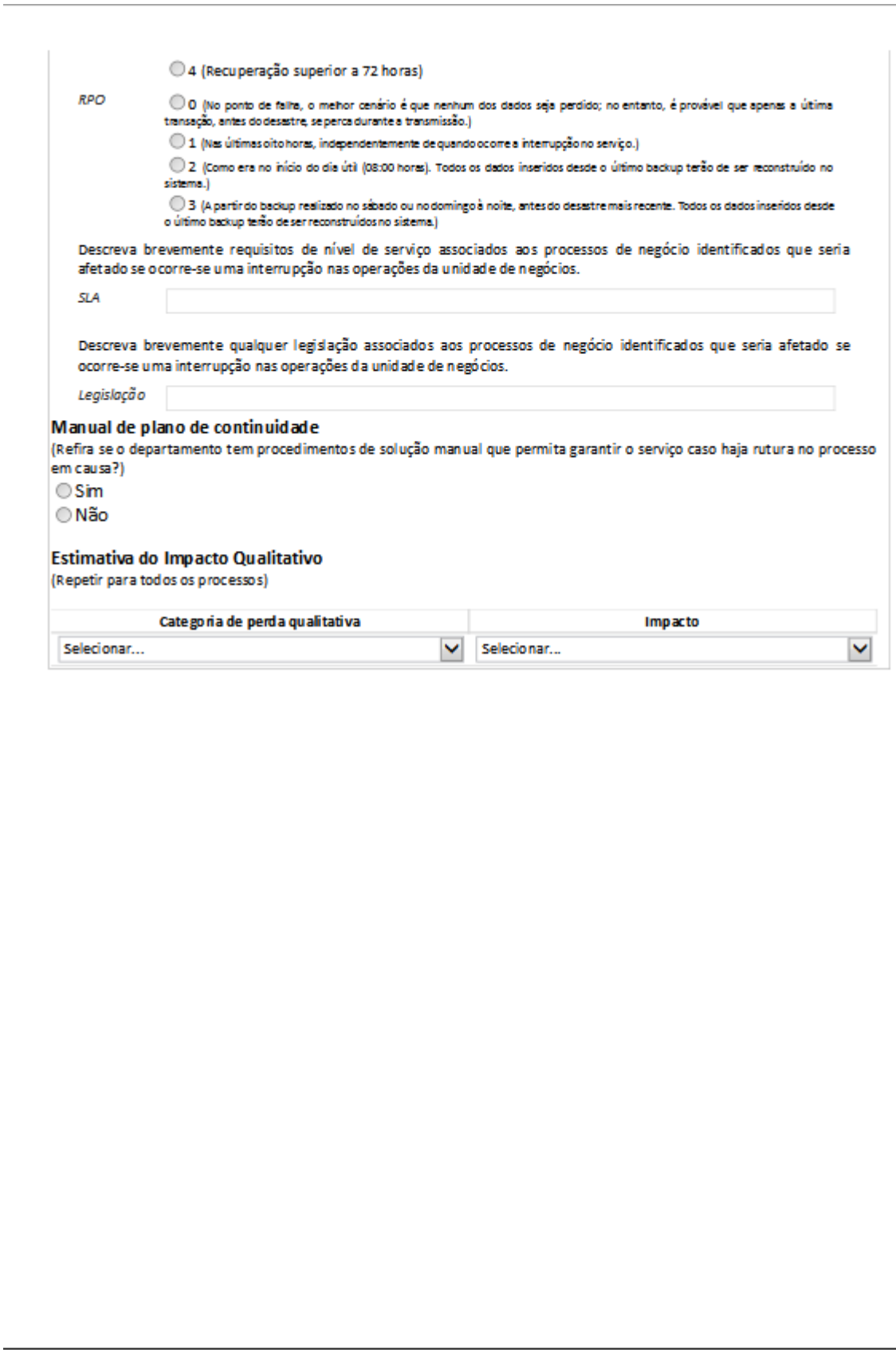
Nome do processo	*Número de Técnicos*	*Frequência do Processo*
Selecionar...		○ Diariamente ○ Semanalmente ○ Mensalmente ○ Trimestralmente ○ Semestralmente ○ Anualmente

Escolher processo:

Para cada processo de negócio, pode haver subprocessos que são concluídos para apoiar o processo de negócio principal. Por favor liste os subprocessos e respetivos RTO e RPO. Se não houver que nenhum subprocessos por favor, deixam esta seção em branco.

RTO

○ 0 (Recuperação em 0 minutos – recuperação imediata)
○ 1 (Recuperação em 24 horas)
○ 2 (Recuperação em 48 horas)
○ 3 (Recuperação em 72 horas)



4 (Recuperação superior a 72 horas)

RPO

0 (No ponto de falha, o melhor cenário é que nenhum dos dados seja perdido; no entanto, é provável que apenas a última transação, antes do desastre, se perca durante a transmissão.)

1 (Nas últimas oito horas, independentemente de quando ocorre a interrupção no serviço.)

2 (Como era no início do dia útil (08:00 horas). Todos os dados inseridos desde o último backup terão de ser reconstruído no sistema.)

3 (A partir do backup realizado no sábado ou no domingo à noite, antes do desastre mais recente. Todos os dados inseridos desde o último backup terão de ser reconstruídos no sistema.)

Descreva brevemente requisitos de nível de serviço associados aos processos de negócio identificados que seria afetado se ocorre-se uma interrupção nas operações da unidade de negócios.

SLA

Descreva brevemente qualquer legislação associados aos processos de negócio identificados que seria afetado se ocorre-se uma interrupção nas operações da unidade de negócios.

Legislação

Manual de plano de continuidade

(Refira se o departamento tem procedimentos de solução manual que permita garantir o serviço caso haja rutura no processo em causa?)

Sim

Não

Estimativa do Impacto Qualitativo

(Repetir para todos os processos)

Categoria de perda qualitativa	Impacto
Selecionar...	Selecionar...

ANEXO 2 – PRÉ-TESTE

Um pré-teste não é mais que uma revisão formal do questionário e da metodologia de recolha de dados que lhe está associada, ou seja, o pré-teste consiste em aplicar o questionário numa subamostra em que é solicitada a colaboração para identificar possíveis problemas.

O pré-teste tem como objetivo verificar a relevância, clareza e compreensão das perguntas aos questionados.

O pré-teste foi realizado com um grupo de seis pessoas, entre 21 de fevereiro e 30 de março de 2013.

Relativamente ao pré-teste foram obtidas as seguintes sugestões:

- Como será difícil estimar custos em euros de eventuais interrupções seria de considerar incluir indicação de como estimar esses custos.
- A principal dificuldade destes questionários é a falta de capacidade dos questionados em responderem considerando que consideram tudo critico e não têm noção dos custos em causa nem do seu impacto na organização como um todo.
- O formato e informação obtida no questionário é a normal em comparação com outros questionários deste género.
- O levantamento tem de ser interativo e, a informação entre os utilizadores e chefias e até mesmo entre departamentos tem de ser constantemente validada.
- Definir uma métrica para a estimativa do impacto quantitativo, como por exemplo em previsão de impacto na deterioração da qualidade ambiental, área ou número de pessoas afetadas.
- O modelo de questionário apresentado, em algumas situações, é mais vocacionado para o negócio das empresas, em concreto na questão relativa ao número de transações e na questão referente à estimativa de impacto qualitativo e quantitativo, nomeadamente no que concerne aos custos uma vez que será difícil apurar montantes considerando a dificuldade em prever receitas.
- Dificuldade no preenchimento por se considerar que não existe um conhecimento suficientemente explicita dos processos de negócio envolvidos na atividade da organização, por parte dos elementos que possam vir a ser entrevistados.
- Foram igualmente detetadas algumas gralhas de escrita.

As sugestões dadas foram tidas em consideração e o questionário foi reformulado, para se obter uma maior precisão, clareza e validade do mesmo.

ANEXO 3 – CENÁRIOS DE ESTRATÉGIAS DE RECUPERAÇÃO DE DESASTRE

Cenário A- Mirror Site Físico-Físico

Descrição da Solução

- Replicação servidores Físico-Físico. Servidores idênticos, com discos "espelhados".
- Replicação do storage por Hardware – exige equipamentos idênticos.
- Exige grande largura de banda, para garantir a replicação em locked step.

Resultados: RPO = 0 RTO= 0

Servidores	**Comutação de Servidores**	Servidores
C7000 5xBL480 com W2K3/8	Rácio 1:1, servidores identicos. Servers fazem boot da SAN. Arranque (a frio) de Blades no Site Secundário, após paragem do Site Primário.	C3000 5xBL480 c/ WK3/8
Armazenamento	**Réplica/Backup**	Armazenamento
EVA 4400	Réplica em locked step do EVA - Contínuous Access. Desvantagem: latência de escrita aumenta, porque tem que confirmar dos 2 EVAS.	EVA 4400, com 3TB úteis
Networking	**Comunicações**	Networking
-	Iplink 10GB ou SanLink 4GB. Com 1Gbps a latência faz-se sentir.	-
Site Primário		Site Secundário

Cenário B- Geocluster Físico-Físico

Descrição da Solução

- Replicação servidores Físico-Físico (ou físico-virtual), através de um software de cluster Geográfico, que não necessita de storage partilhado.
- Volumes de Sistema e de dados são copiados pelo Geocluster entre sites.
- Exemplo de Geoclusters: **Symantec VRTS Storage Foundation HA/DR; Double-take Recovery Now; Faconstor Continuos Data Protection**

Resultados: RPO < 1h RTO= 1h

Site Primário		Site Secundário
Servidores	**Comutação de Servidores**	Servidores
C7000 5xBL480 com W2K3/8	Rácio 1:1, entre hardware dissimilar. Variante Geocluster F-V permite 2:1.	5xDL380 c/ WK3/8 rácio 1:1
Armazenamento	**Réplica/Backup**	Armazenamento
EVA 4400	Geocluster produz cópias de-duplicadas dos volumes dos servidores windows.	Storage distinto. Ex: MSA 2000
Networking	**Comunicações**	Networking
-	IPlink 1Gbps, ou 100Mbps com aceleração WAN (ex:Riverbed)	-

Cenário C- Backup+Failover Site Físico-Físico

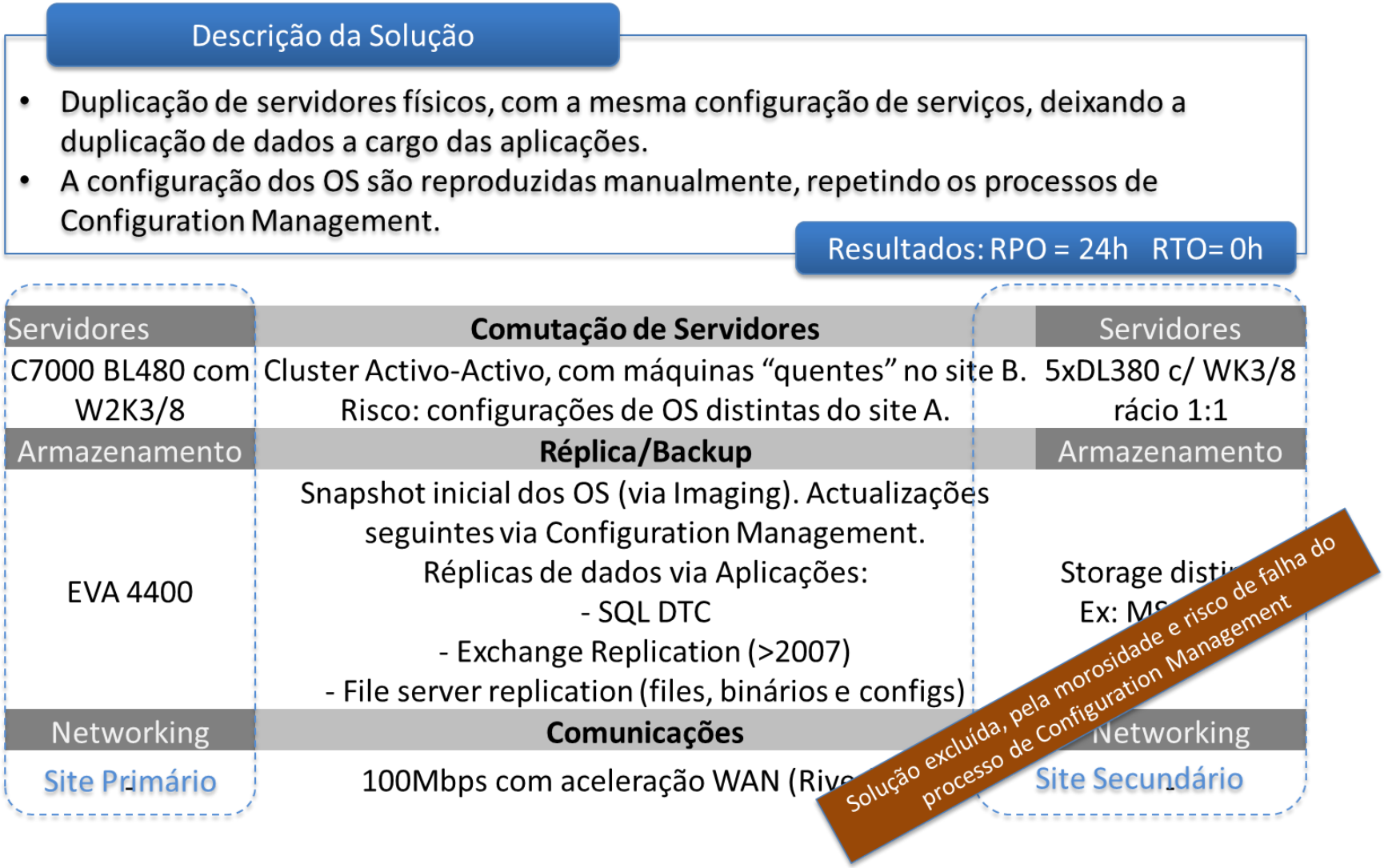
Descrição da Solução

- Replicação servidores Físico-Físico, num modelo BTRR (Backup-Transport-Restore-Recover)
- Sistemas operativos transferidos via **Symantec System Restore**, permitindo recuperação em hardware dissimilar, no site secundário.
- Backup de dados transferido para site secundário, e recuperado em caso de necessidade.

Resultados: RPO = 24h RTO = 8h

Servidores	**Comutação de Servidores**	Servidores
C7000 BL480 com W2K3/8	Reposição de OS com System Restore, seguido de reposição dos Backups de Dados.	5xDL380 c/ WK3/8 rácio 1:1
Armazenamento	**Réplica/Backup**	**Armazenamento**
EVA 4400	Backup de sistemas via Symantec System Restore. Backup de Dados via Symantec VRTS Backup.	Storage distinto. Ex: MSA 2000
Networking	**Comunicações**	**Networking**
-	100Mbps com aceleração WAN (Riverbed)	-
Site Primário		Site Secundário

Cenário D- Replicação ao nível Aplicacional



Cenário E- Geocluster Virtual-Virtual

Descrição da Solução

- Replicação servidores Virtual-Virtual, por réplica dos volumes VMFS com as máquinas virtuais entre o Site A e Site B.
- **Vmware SRM** orquestra recuperação de Hosts no Site B.
- Replicação do storage por Hardware – exige equipamentos idênticos.
- Exige grande largura de banda, para garantir a replicação em locked step.

Resultados: RPO = 0 RTO= 0

Servidores	**Comutação de Servidores**	Servidores
C7000 BL480 com W2K3/8	rácio 2:1 de hosts físicos, assumindo que redução de performance é aceitável em Contingência	3xDL380 c/ Vmware
Armazenamento	**Réplica/Backup**	Armazenamento
EVA 4400	Réplica do EVA em locked step - Continuous Access. Downside: latência de escrita aumenta, porque tem que confirmar dos 2 EVAS.	EVA 4400
Networking	**Comunicações**	Networking
-	Iplink 10GB ou SanLink 4GB. Com 1Gbps a latência faz-se serntir.	-
Site Primário		Site Secundário

Cenário F- Backup+Failover Virtual-Virtual

Descrição da Solução

- Replicação servidores Virtuais, num modelo BTRR (Backup-Transport-Restore-Recover)
- Backup de máquinas virtuais, com transferência para Site B.
- Descompressão Manual dos backups para imagens VMFS, e arranque dos servidores Virtuais via Virtualcenter

Resultados: RPO = 24 RTO= 4

Servidores	**Comutação de Servidores**	Servidores
C7000 BL480 com W2K3/8	rácio 2:1 de hosts físicos, assumindo que redução de performance é aceitável em Contingência	3xDL380 c/ WK3/8 rácio 1:1
Armazenamento	**Réplica/Backup**	Armazenamento
EVA 4400	Backup Volumes Vmware via WAN para o Site Backup. Sistemas **Veeam; Commvault**.	Storage distinto. Ex: MSA 2000
Networking	**Comunicações**	Networking
-	100Mbps com acelaração WAN (Riverbed)	-
Site Primário		Site Secundário

Cenário G- Geoclusters Cloud

Descrição da Solução

- Replicação servidores Físicos ou Virtuais, através de um software de cluster Geográfico, que não necessita de storage partilhado, para servidores numa Cloud Pública.
- Volumes de Sistema e de dados são copiados pelo Geocluster para os servidores na Cloud.

Resultados: RPO = 8h RTO= 1h

Servidores	**Comutação de Servidores**	Servidores
C7000 BL480 com W2K3/8	Servidores na Cloud.	Cloud Servers Ex :Amazon E2C
Armazenamento	**Réplica/Backup**	Armazenamento
EVA 4400	Cópias deduplicadas dos Hosts P ou V para Storage Delivery Networks (SDN). Exemplo de Geoclusters Cloud: **Doubletake+Amazon AWS; Doyenz; Nirvanix+Commvault; Zenith**	Cloud Storage Ex: Amazon AWS
Networking	**Comunicações**	Networking
Site Primário	Internet link com Upload de 100Mbps	Site Secundário

ANEXO 5 – CONSIDERAÇÕES ADICIONAIS DOS CENÁRIOS

Atividades do Recovery Management

- Comutação DNS
    - Registo Web
    - Registo MX
- Confirmar os portos abertos do Firewall do «*site*» secundário
- Reconfigurar serviço de «*anti-spam*», caso seja serviço externo
- Alteração dos IPs dos servidores «*site*» secundário (imagens têm IPs «*site*» primário)
- Confirmar se há licenciamento preso ao IP, em cujo caso tem que se atualizar
- Comutação de «*layers*» de rede:
    - Se no «*site*» primário há um balanceador de carga (NLB), este tem que ser recriado no «*site*» Secundário («*hardware*» ou NLB)
- Criação de mecanismos temporários de «*Backup*», para o caso da contingência se prolongar
- Preparar mecanismo de reserva, para retomar operação no «*site*» Principal, após recuperação de desastre.

Atividades para Acesso dos Utilizadores

- Ativação de concentrador VPN, para acesso remoto dos utilizadores de contingência
- Preparação prévia:
- Utilizadores com mecanismos de acesso (placas 3G, clientes VPN)
- Formação
- Idealmente servidor de RDP/VDI para facilitar acesso a aplicações de qualquer posto

ANEXO 4 - PILOTO TECNOLÓGICO

Objetivos do Piloto:

- Confirmar que as soluções apontadas cumprem os níveis de RTO e RPO exigidos pela Organização, para as condições de largura de banda e de *"hardware»* no *"site»* de recuperação
- Comparar entre duas soluções «*Geocluster*» líderes, para recomendar uma delas (avaliação tecnológica)
- Definir os parâmetros de configuração concretos da solução escolhida, bem como a arquitetura de sistemas e comunicações
- Produzir especificação técnica para constar em caderno de encargos

Ambiente do Piloto:

O Piloto decorrerá nas instalações da organização, já que é inviável contratar ligações de comunicação por um prazo de 1 mês.

Assim torna-se necessário implementar um laboratório com um simulador de rede WAN (para simular o comportamento com diferentes largura de banda), a interligar o ambiente de Produção e um ambiente secundário (*"site»* B). Tudo isto no Centro de computação da Organização.

O Piloto será realizado para a totalidade das aplicações a salvaguardar.

O Piloto vai testar 2 soluções de «*Geocluster»*, pelo que repetirá os testes com 2 ambientes distintos.

O Ambiente Secundário deverá ser fornecido pela organização: 3 servidores «*Rack*» ou «*Blade*» e um *Storage* MSA2000 ou equivalente com 3 TB de dados.

Tarefas e Entregáveis:

- Preparar equipamento simulador WAN;
- Configuração do Hardware do *"site»* B
- Piloto *Geocluster Symantec*
- Configurar *Geocluster Symantec* (inclui consultores *Symantec*)
- Iniciar Replicação «*Sites*»
- Comprovar balanceamento (fim de semana)
- Piloto «*Geocluster Double-take*»
- Configurar «*Geocluster Symantec*» (inclui consultores «*Double-take*»)
- Iniciar Replicação Sites
- Comprovar balanceamento (fim de semana)
- Documento comparativo entre Solução «*Symantec»* e «*Double-take»*, incluindo comparação entre aspetos Tecnológicos, Funcionalidades, Qualidade do suporte, desempenho no Piloto, «*roadmap*» conhecido para o produto.

Apresentação à Organização

Documento de Especificações técnicas para a solução escolhida, para incluir no Caderno de Encargos: comunicações, plataforma de *"hardware»*, especificação do «*Geocluster»*, requisitos para a configuração.

Cronograma:

O Piloto terá uma duração de 7 semanas (as duas plataformas não podem ser feitas em paralelo).