

**MESG**  
**MESTRADO EM ENGENHARIA**  
**DE SERVIÇOS E GESTÃO**

**A Continuidade do Negócio no sistema hospitalar português:  
retrato actual e metodologia aplicada no desenvolvimento de um  
plano**

*Manuel Vítor de Lima Vieira Alves*

**Relatório de Dissertação**

Orientador: Prof. Doutor António Ernesto da Silva Carvalho Brito



Universidade do Porto

Faculdade de Engenharia

**FEUP**

**Faculdade de Engenharia da Universidade do Porto**

2010-07-20



*À Raquel, minha companheira de jornada, que com “longa paciência” me acompanha nesta inquietude pelo conhecimento.*



## Resumo

Com grande regularidade somos confrontados com notícias de tempestades, terremotos, incêndios, falências, crises, com impacto nas pessoas e nas organizações. A recente catástrofe com a plataforma petrolífera no Golfo do México ou impacto desastroso do vulcão islandês Eyjafjallajökull na circulação aérea, pelas suas consequências directas e indirectas, alertam-nos para a necessidade da existência de uma política de gestão da continuidade do negócio que auxilie as organizações a minimizar o seu impacto, na impossibilidade de evitar a sua ocorrência. A gestão da continuidade do negócio tem como objectivo principal evitar, ou reduzir sensivelmente, as perdas das organizações em casos de incidentes que afectem suas operações, além de restaurar suas actividades no espaço de tempo mais breve possível. Esta política é seguida com grande acuidade no mundo anglo-saxónico mas não é acompanhada na generalidade das organizações portuguesas, excepção das grandes empresas dos sectores financeiro, seguros e telecomunicações. O objecto deste estudo é analisar os principais vectores de uma política de gestão da continuidade do negócio e estabelecer um retrato actual da sua implementação nos hospitais portugueses. Para atingir este objectivo foi efectuada uma sondagem junto de 108 hospitais públicos, privados e do sistema social, através de questionários. A investigação demonstra que, apesar da elevada importância (98%) atribuída a esta política, 83% dos hospitais não dispõe de um plano de continuidade, 78% não implementou um plano de recuperação de desastres e 15% ainda não dispõe de um plano de emergência. Complementando este estudo apresenta-se uma metodologia de desenvolvimento de um plano de continuidade em resultado de um caso de estudo desenvolvido num hospital.

**Palavras-chave:** Gestão da Continuidade do Negócio, Plano de Continuidade do Negócio, Plano de Recuperação de Desastres, Risco, Análise de Impacto no Negócio, Maturidade dos Sistemas de Informação,



## **The Business Continuity Management in Portuguese hospital system: the current picture and the methodology applied in developing a plan**

### **Abstract**

*With great regularity we are confronted with news of storms, earthquakes, fires, bankruptcies, crises, which impacts on people and organizations. The recent disaster on the oil platform in the Gulf of Mexico or disastrous impact of the Icelandic volcano Eyjafjallajökull in air travel, for their direct and indirect consequences, warn us of the need for the existence of a policy for business continuity management that helps organizations to minimize its impact, failing to prevent their occurrence. The business continuity management has as main objective to avoid or substantially reduce the losses of the organizations in cases of incidents affecting their operations, and restore their activities within the shortest time possible. This policy is followed with great accuracy in the Anglo-Saxon world but is not accompanied in most of the Portuguese organizations, except large companies in the financial sector, insurance and telecommunications. The purpose of this study is to analyze the main elements of a policy for business continuity management and establish a current picture of its implementation in Portuguese hospitals. To achieve this objective was carried out a survey of 108 public hospitals, private and social system, through questionnaires. Research shows that despite the high importance (98%) attributed to this policy, 83% of hospitals do not have a continuity plan, 78% had not implemented a disaster recovery plan and 15% still do not have a emergency plan. Complementing this study presents a methodology for developing a business continuity plan as a result of a case study done in a hospital.*

**Keywords:** *Business Continuity Management, Business Continuity Plan, Disaster Recovery Plan, Risk Analysis, Business Impact Analysis, Maturity of Information Systems*



## Agradecimentos

*“Em tudo sede agradecidos, ...” (I Ts 5:18)*

Agradeço ...

... à minha mulher Raquel, pelo amor, estímulo, acreditar, ..., e pela longa paciência nesta renovada aventura formativa.

... aos meus filhos Cláudio e Priscila, colegas engenheiros, pelo carinho, entusiasmo e incentivo.

... aos demais familiares, amigos e colegas pelo persistente apoio e incentivo.

... ao meu orientador Prof. Doutor António Carvalho Brito, pelo duto e experiente saber partilhado, incentivo, colaboração no desenvolvimento do caso de estudo e pela orientação no desenvolvimento do projecto de dissertação.

... aos excelentes e dedicados professores do MESH com quem tive o prazer de muito aprender e que muito contribuíram para esta experiência extraordinária e apaixonante, e para o sucesso desta pós-graduação.

... aos meus colegas do MESH com quem vivi momentos de descoberta fantásticos e cujo saber, maturidade, empenho e generosidade na partilha é um crédito inegociável.

... à DGITA, na pessoa dos seus dirigentes Dr.<sup>a</sup> Ana Moraes, Dr. João Reynaud e Eng.<sup>o</sup> Luís Encarnação pelas condições disponibilizadas para a frequência do Mestrado.

... ao Hospital da Prelada, na pessoa do seu administrador Dr. Joaquim Faria e Almeida e demais colaboradores – Dr. Jorge Lima e Eng.<sup>o</sup> João Figueiredo, pela incansável disponibilidade e colaboração, Carlos Marques, José Manuel Rocha, Dr.<sup>a</sup> Julieta Quintas, pela colaboração nas entrevistas.

... aos Dr.<sup>a</sup>. Fernandina Oliveira, Dr. Serafim Carvalho e Eng. Tiago Moraes da Unidade Local de Saúde de Matosinhos pela disponibilidade em facultarem as informações solicitadas e o seu tempo.

... à Cláudia Lopes pela partilha dos resultados do seu estudo sobre a implementação do Sistema Integrado de Gestão de Inscritos para Cirurgia – SIGIC no Hospital da Prelada.

... à colega doutoranda Albertina Medeiros, ao Prof. Doutor Augusto Fernandes e à administração da AMBITAT pelas experiências com a metodologia criativa.

... ao Prof. Doutor Luís Velez Lapão pela partilha de informação sobre os Sistemas de Informação da Saúde.

... à Raquel, Priscila e Pedro pela ajuda na revisão do texto.

... à Francisca pela colaboração no insistente contacto com os hospitais.

... aos hospitais portugueses que acederam participar no questionário.

... a todos que directa e indirectamente contribuíram de alguma forma para o sucesso desta aprendizagem!

Muito obrigado!



*"Os conhecimentos dão-nos meios para viver.  
A sabedoria dá-nos razões para viver.  
Sábias são as pessoas que sabem viver.  
Tolo é aquele que, tendo defendido tese sobre  
barcos e mapas, não sonha com horizontes,  
não planeia viagens, não imagina portos..."*

Rubem Alves in "Livro sem fim"



## Conteúdos

|         |                                                                                   |    |
|---------|-----------------------------------------------------------------------------------|----|
| 1       | Introdução.....                                                                   | 1  |
| 1.1     | Motivação do estudo.....                                                          | 2  |
| 1.2     | Objectivo do estudo .....                                                         | 3  |
| 1.3     | Delimitação do estudo.....                                                        | 3  |
| 1.4     | Estrutura do estudo.....                                                          | 4  |
| 2       | Enquadramento Teórico.....                                                        | 5  |
| 2.1     | As Organizações baseadas na Informação .....                                      | 5  |
| 2.1.1   | Os Sistemas de Informação hospitalar .....                                        | 9  |
| 2.2     | O Risco nas Organizações .....                                                    | 11 |
| 2.3     | Gestão da Continuidade do Negócio.....                                            | 14 |
| 2.3.1   | Dimensões da Gestão da Continuidade do Negócio .....                              | 16 |
| 2.3.2   | Abordagens na implementação da Gestão da Continuidade do Negócio .....            | 20 |
| 2.3.2.1 | Plano de Emergência .....                                                         | 22 |
| 2.3.2.2 | Plano de Recuperação de Desastres .....                                           | 23 |
| 2.3.2.3 | Plano de Continuidade do Negócio .....                                            | 26 |
| 2.4     | Gestão da Continuidade do Negócio no contexto hospitalar .....                    | 27 |
| 3       | Um retrato da continuidade do negócio nos hospitais em Portugal: Metodologia..... | 31 |
| 3.1     | Abordagem Metodológica.....                                                       | 31 |
| 3.2     | Universo e amostra .....                                                          | 32 |
| 3.3     | Recolha de dados .....                                                            | 33 |
| 3.4     | Processamento dos dados .....                                                     | 33 |
| 3.5     | Limitações do método .....                                                        | 33 |
| 3.6     | Considerações Éticas.....                                                         | 34 |
| 4       | Um retrato da continuidade do negócio nos hospitais em Portugal: Análise .....    | 35 |
| 4.1     | Dimensão através do n.º de camas de internamento .....                            | 36 |
| 4.2     | Valências de Serviço.....                                                         | 37 |
| 4.3     | Maturidade dos sistemas de informação hospitalares .....                          | 39 |
| 4.4     | Importância da Continuidade do Negócio no serviço hospitalar.....                 | 42 |
| 4.5     | Percepção dos Riscos potenciais .....                                             | 42 |
| 4.6     | Quebras de Serviço e Impacto no Negócio .....                                     | 44 |
| 4.7     | Plano de Continuidade do Negócio e os seus componentes.....                       | 45 |
| 4.8     | Plano de Recuperação dos Desastres .....                                          | 49 |
| 4.8.1   | Políticas de segurança da informação digital .....                                | 50 |
| 4.9     | Plano hospitalar de Emergência .....                                              | 51 |
| 5       | Metodologia aplicada no desenvolvimento de um plano de continuidade.....          | 53 |
| 5.1     | Os standards internacionais para a Gestão da Continuidade do Negócio.....         | 53 |
| 5.1.1   | <i>Disaster Recovery Institute International – DRII</i> .....                     | 53 |
| 5.1.2   | <i>British Standard Institute – BSI</i> .....                                     | 54 |
| 5.1.3   | <i>IT Information Library – ITIL</i> .....                                        | 56 |
| 5.1.4   | <i>Control Objectives for Information and related Technology – COBIT</i> .....    | 59 |
| 5.2     | Caracterização do serviço hospitalar .....                                        | 60 |

|       |                                                                                                                          |    |
|-------|--------------------------------------------------------------------------------------------------------------------------|----|
| 5.2.1 | Missão, Visão e Valores .....                                                                                            | 61 |
| 5.2.2 | Estrutura Organizacional .....                                                                                           | 61 |
| 5.2.3 | Modelo de Negócio.....                                                                                                   | 61 |
| 5.3   | Âmbito de aplicação da metodologia .....                                                                                 | 63 |
| 5.4   | Metodologia aplicada no desenvolvimento do plano.....                                                                    | 63 |
| 5.4.1 | Governança .....                                                                                                         | 63 |
| 5.4.2 | Programa de Acção.....                                                                                                   | 65 |
| 5.4.3 | Análise do Impacto no Negócio.....                                                                                       | 65 |
| 5.4.4 | Avaliação do Risco.....                                                                                                  | 69 |
| 5.4.5 | Elaboração do <i>BCP</i> .....                                                                                           | 71 |
| 5.4.6 | Monitorização do Risco e Teste .....                                                                                     | 73 |
| 6     | Conclusões.....                                                                                                          | 75 |
|       | Referências e Bibliografia .....                                                                                         | 77 |
|       | Anexo A – Inquérito sobre a Gestão de Continuidade do Negócio nos hospitais portugueses –<br>carta de apresentação ..... | 80 |
|       | Anexo B – Inquérito sobre a Gestão de Continuidade do Negócio nos hospitais portugueses.....                             | 81 |
|       | Anexo C – Standards Internacionais relacionados com <i>BCM</i> .....                                                     | 86 |
|       | Anexo D - Organograma do Hospital da Prelada Dr. Domingos Braga da Cruz .....                                            | 88 |
|       | Anexo E - Arquitectura do Sistema de Prestação de Serviço.....                                                           | 89 |
|       | Anexo F – Processos de Negócio .....                                                                                     | 92 |
|       | Anexo G - Análise de Impacto no Negócio – Processos – Questionário.....                                                  | 93 |
|       | Anexo H – Análise de Impacto no Negócio – Sistemas – Questionário.....                                                   | 97 |
|       | Anexo I – Imagens da <i>Workshop</i> “Identificando Riscos, Construindo Alternativas” .....                              | 98 |
|       | Anexo J – Matriz de Análise de Vulnerabilidades .....                                                                    | 99 |

## Lista de Figuras

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Figura 1 - Evolução das estruturas de redes. ....                     | 6  |
| Figura 2 - Informação Criada, Capturada e Replicada.....              | 7  |
| Figura 3- O Processo de Negócio. ....                                 | 7  |
| Figura 4 - Elementos da Organização Integrada .....                   | 8  |
| Figura 5 - Componentes do Hospital Digital.....                       | 10 |
| Figura 6 - Eventos disruptivos dos SI.....                            | 14 |
| Figura 7 - Matriz de Vulnerabilidade.....                             | 14 |
| Figura 8 - Dimensões da Gestão de Continuidade do Negócio.....        | 16 |
| Figura 9 - Processo unificador.....                                   | 18 |
| Figura 10 - Componentes da Gestão de Continuidade do Negócio.....     | 21 |
| Figura 11 - Abordagens da continuidade. ....                          | 21 |
| Figura 12 - Processo de Recuperação. ....                             | 25 |
| Figura 13 - Relação de questionários enviados e recebidos.....        | 35 |
| Figura 14 - N.º de Camas por Natureza de hospital.....                | 37 |
| Figura 15 - Oferta de Cuidados de Saúde pelas diversas valências..... | 38 |
| Figura 16 - Distribuição das valências por natureza de hospital ..... | 38 |
| Figura 17 - Maturidade dos SI nos Hospitais Portugueses.....          | 39 |
| Figura 18 - Comparação da Maturidade dos SI no Hospitais.....         | 40 |
| Figura 19 - Percepção do Risco no Negócio Hospitalar .....            | 43 |
| Figura 20 - Importância do Plano de Continuidade do Negócio .....     | 45 |
| Figura 21 - Implementação de um Plano de Continuidade .....           | 46 |
| Figura 22 – BSI2599 BCM Program .....                                 | 55 |
| Figura 23 - Biblioteca ITIL .....                                     | 57 |
| Figura 24 - Metodologia ITSCM.....                                    | 58 |
| Figura 25 - COBIT 4.1.....                                            | 59 |
| Figura 26 - Constelação de Valor dos Cuidados de Saúde .....          | 62 |
| Figura 27 - Principais Áreas de Negócio do HP.....                    | 62 |
| Figura 28 - As fases de desenvolvimento do BCP .....                  | 63 |
| Figura 29 - Máximo Período Tolerável de Disrupção. ....               | 66 |
| Figura 30 - Processos de Negócio do HP.....                           | 67 |
| Figura 31 – Arquitectura do Sistema de Prestação de Serviço.....      | 67 |

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| Figura 32 – Matriz de Interdependências entre Processos, Participantes e Plataforma ..... | 68 |
| Figura 33 - Matriz de Criticidade das Aplicações / Sistemas.....                          | 68 |
| Figura 34 - Estratégia no desenvolvimento de um BCP .....                                 | 72 |

## Lista de Tabelas

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Tabela 1 - Matriz de Análise de Vulnerabilidade.....                                 | 23 |
| Tabela 2 - Hospitais seleccionados por sector.....                                   | 33 |
| Tabela 3 - Questionários enviados e recebidos .....                                  | 35 |
| Tabela 4 - N.º oficial de camas por natureza de hospital .....                       | 36 |
| Tabela 5 - Representação da dimensão por tipo de hospital .....                      | 36 |
| Tabela 6 - Distribuição de Valências de Serviço por natureza de hospital.....        | 37 |
| Tabela 7 - Comparação da Maturidade dos SI no Hospitais .....                        | 39 |
| Tabela 8 – Taxa de Implementação das Aplicações nos Hospitais .....                  | 40 |
| Tabela 9 - <i>Ranking</i> das Soluções de TI.....                                    | 41 |
| Tabela 10 – Grau de Importância da Gestão da Continuidade do Negócio .....           | 42 |
| Tabela 11 - Condução da Política de BCM.....                                         | 42 |
| Tabela 12 - Percepção do Risco.....                                                  | 43 |
| Tabela 13 - Registo de Quebras de Serviço .....                                      | 44 |
| Tabela 14 - N.º de dias de quebras de serviço registados .....                       | 44 |
| Tabela 15 - Causas das Quebras de Serviço e n.º de ocorrências.....                  | 44 |
| Tabela 16 - Riscos cobertos pelos Planos de Continuidade de Negócio .....            | 45 |
| Tabela 17 - Importância da existência de um BCP.....                                 | 46 |
| Tabela 18 - Recursos Técnicos envolvidos e sua natureza .....                        | 46 |
| Tabela 19 - Previsão de Implementação de um BCP.....                                 | 47 |
| Tabela 20 - Justificação do adiamento da decisão .....                               | 48 |
| Tabela 21 - Análise de Impacto no Negócio .....                                      | 48 |
| Tabela 22 – Existência de DRP .....                                                  | 49 |
| Tabela 23 - Periodicidade na revisão do DRP.....                                     | 49 |
| Tabela 24 - Periodicidade dos <i>Backups</i> .....                                   | 50 |
| Tabela 25 – Confiabilidade dos <i>Backups</i> e Procedimentos de Recuperação .....   | 50 |
| Tabela 26 - Localização dos <i>Backups</i> .....                                     | 50 |
| Tabela 27 – Planos de Emergência: Existência e Perspectivas de desenvolvimento. .... | 51 |
| Tabela 28 - Regularidade nos Testes dos Planos de Emergência.....                    | 51 |
| Tabela 29 – BS25999-2 Fases e Actividades do Sistema de BCM .....                    | 56 |
| Tabela 30 - Causas e Consequências da Falta de Suporte no Programa de BCP .....      | 64 |
| Tabela 31 - Áreas e Processos de Negócio do HP.....                                  | 66 |

Tabela 32 - Tabela de Ameaças ..... 70

Tabela 33 - Tabela de Ameaças mais prováveis..... 70

Tabela 34 - Cenário, Probabilidade e Impacto das Ameaças ..... 71

**Lista de Abreviaturas**

|       |                                                           |
|-------|-----------------------------------------------------------|
| ADME  | Assistência na Doença dos Militares do Exército           |
| ADSE  | Assistência na Doença dos Servidores do Estado            |
| AMP   | Atendimento Médico Permanente                             |
| BCI   | Business Continuity Institute                             |
| BCM   | Business Continuity Management                            |
| BCP   | Business Continuity Planning                              |
| BIA   | Business Impact Analysis                                  |
| BSI   | British Standards Institute                               |
| CICS  | Customer Information Control System                       |
| CMMI  | Capability Maturity Model Integration                     |
| COBIT | Control Objectives for Information and related Technology |
| CPOE  | Computerized Physician Order Entry                        |
| CRD   | Clinical Data Record                                      |
| DRII  | Disaster Recovery Institute International                 |
| DRP   | Disaster Recovery Planning                                |
| EMR   | Electronic Medical Record                                 |
| EP    | Emergency Planning                                        |
| EPE   | Entidade Pública Empresarial                              |
| HIS   | Healthcare Information Systems                            |
| HP    | Hospital da Prelada Dr. Domingos Braga da Cruz            |
| HQS   | Health Quality Service                                    |
| HVAC  | Heating, Ventilation and Air Conditioning                 |
| ISO   | International Organization of Standardization             |
| ITIL  | Information Technology Infrastructure Library             |
| ITSCM | Information Technology Service Continuity Management      |
| LAN   | Local Area Network                                        |
| LISS  | Laboratory Information System                             |
| MCDT  | Meios Complementares de Diagnóstico e Tratamento          |
| PACS  | Picture Archiving and Communication System                |
| RAID  | Redundant Array of Independent Disks                      |
| RISS  | Radiology Information System                              |

---

|       |                                                        |
|-------|--------------------------------------------------------|
| RPO   | Recovery Point Objective                               |
| RTO   | Recovery Time Objective                                |
| SCMP  | Santa Casa da Misericórdia do Porto                    |
| SI    | Sistemas de Informação                                 |
| SIGIC | Sistema Integrado de Gestão de Inscritos para Cirurgia |
| SNS   | Serviço Nacional da Saúde                              |
| SSA   | Service System Architecture                            |
| TI    | Tecnologias de Informação                              |
| TIC   | Tecnologias de Informação e Comunicação                |
| UCCI  | Unidade de Cuidados Continuados Intensivos             |
| WAN   | Wide Area Network                                      |

## Glossário

**ACTIVO:** Item da propriedade e/ou componente do processo de negócio da pertença da organização. Os activos distinguem-se por: activos físicos (p.e. edifícios, equipamentos); activos financeiros (p.e. moeda, depósitos bancários, acções); activos intangíveis (p.e. *goodwill*, reputação, marca)

**ALERTA:** Notificação formal de que um incidente/desastre ocorreu e que deve desencadear uma invocação do Plano de Continuidade do Negócio ou do Plano de Emergência.

**AMEAÇA:** a causa potencial de um incidente, do qual pode resultar prejuízo no sistema ou na organização.

**ANÁLISE DE IMPACTO NO NEGÓCIO:** Análise ao nível da gestão através da qual a organização avalia os impactos quantitativos (financeiros) e qualitativos (não financeiros), os efeitos e as perdas que poderiam resultar se a organização quebrasse o serviço. Os resultados da AIN são utilizados para tomar decisões sobre a estratégia de continuidade do negócio e soluções.

**AUDITORIA:** Processo em que procedimentos e/ou documentação são confrontados com standards estabelecidos.

**COMITÉ DE CONTINUIDADE:** Conjunto de papéis e responsabilidades definidos para a implementação de um Plano de Continuidade do Negócio.

**GESTÃO DE RISCOS (dos Sistemas de Informação):** processo de identificar, controlar e minimizar ou eliminar os riscos de segurança que podem afectar os sistemas de informação, a um custo aceitável.

**BACKLOG:** O efeito sobre os negócios resultante da acumulação de trabalho em resultado de um sistema ou processo estarem indisponíveis por um período inaceitável. A situação em que uma acumulação de trabalho exige mais tempo para a recuperação do que o disponível através dos padrões normais de trabalho. Em circunstâncias extremas, o *backlog* pode tornar-se tão marcante que o atraso não pode ser recuperado.

**BACKUP:** O processo através do qual os dados, electrónicos ou em suporte papel, são copiados de forma a estarem disponíveis e utilizáveis se os dados originais no caso deste se perderem, destruírem ou ficarem corrompidos.

**GESTÃO DA CONTINUIDADE DO NEGÓCIO:** Um processo holístico de gestão que identifica potenciais impactos que ameaçam a organização e fornece um enquadramento para a construção de resiliência e da capacidade para uma resposta efectiva que proteja os interesses dos *stakeholders*, a reputação, a marca e as actividades criadoras de valor.

**GESTÃO DA CONTINUIDADE DO NEGÓCIO- CICLO DE VIDA:** O conjunto de actividades e processos divididos em diversas etapas que são necessárias na gestão da continuidade do negócio.

**INCIDENTE:** é qualquer evento que não faz parte do funcionamento standard de um serviço e que provoca ou pode provocar uma interrupção no serviço ou uma redução na respectiva qualidade.

**INFORMAÇÃO:** é o significado construído a partir dos dados, ou seja, são dados em contexto, com relevância e propósito.

**PLANO DE GESTÃO DE CONTINUIDADE DO NEGÓCIO:** Plano bem definido e documentado a ser utilizado numa emergência, evento, desastre, incidente, crise na gestão do negócio. O plano deve estabelecer quais os recursos, pessoas, serviços e acções necessárias na gestão de um processo de continuidade do negócio.

**POLÍTICA DE GESTÃO DE CONTINUIDADE DO NEGÓCIO:** Define os objectivos da organização, os princípios e a abordagem de continuidade e como ela será garantida, os papéis e as responsabilidades fundamentais, e a forma de governo da continuidade e o seu reporte.

**RISCO (em Segurança da Informação):** é a possibilidade de uma ameaça explorar vulnerabilidades de um activo ou conjunto de activos, do qual pode resultar prejuízo no sistema. É medido em termos de combinação da probabilidade de um evento ocorrer (ex. uma ameaça explorar vulnerabilidades) e as perdas ou prejuízos causados num activo ou grupo de activos.

**VULNERABILIDADE:** fraqueza de um activo ou conjunto de activos, que pode ser explorada por uma ou mais ameaças.

## 1 Introdução

Vivemos tempos de instabilidade e de insegurança! Dito desta forma, esta frase parece provida de um senso comum de alarme e de caracterização do presente que o distinguirá, negativamente, face a outros períodos da história da humanidade. Nada de mais errado e enviesado. O homem, no seu percurso evolutivo, depara-se com novos contextos socioeconómicos de maior exigência a que tem de dar resposta satisfatória. Esta realidade não obsta, no entanto, à crescente preocupação na sustentabilidade das organizações face aos riscos que assolam as diversas comunidades. Fenómenos como a imprevisibilidade da actividade sísmica, vulcânica, climática em geral, acção terrorista, a emergência de pandemias, são exemplo dos desafios às organizações na sustentabilidade dos seus objectivos e na minimização do seu impacto económico e social.

As organizações, fenómeno resultante do encontro de homens e máquinas, são “uma entidade social, conscientemente coordenada, gozando de fronteiras delimitadas que funcionam numa base relativamente contínua, tendo em vista a realização de objectivos comuns” (Bilhim 2004). Independentemente da natureza jurídica, são um bem social essencial para o funcionamento das sociedades e de cujo regular funcionamento depende a humanidade na construção de sociedades justas, democráticas e geradoras de bem-estar.

No funcionamento das organizações, os Sistemas de Informação (SI) são elementos funcionais de que dependem para a continuidade e sucesso dos seus objectivos (Santos 2007). Em 2008, as empresas americanas gastaram cerca de 840 mil milhões de dólares em tecnologias de informação e comunicação (Laudon and Laudon 2009). Em Portugal, de acordo com a IDC (IDC 2009) o mercado de Tecnologias de Informação e Comunicação (TIC) atingiu em 2008 o valor de 3,05 mil milhões de euros, com um crescimento de 11,2 por cento face a 2007. A procura da eficiência económica nas organizações e as alterações das diversas propostas de valor para o cliente são factores que levam as organizações à desmaterialização de processos, melhorando o seu desempenho e proporcionando aos seus clientes novos canais de prestação do serviço. Cada vez mais os SI assumem um papel estratégico e relevante, tornando-se vitais para a organização.

Caso particular deste processo de transferência de tecnologias é o mercado da Saúde. A crescente informatização dos serviços médico - hospitalares no encalço de um anterior processo de informatização dos sistemas de diagnóstico, é uma tendência marcante e solidamente instituída nesse mercado, seja através da oferta pública, privada ou social. A maturidade dos sistemas de informação nas organizações de cuidados de saúde rumo, a passos largos, para a constituição de hospitais virtuais em que todos os processos assentam em tecnologias de informação e comunicação, com a implementação do paradigma da interoperabilidade de sistemas.

Nesse contexto, todos os esforços possíveis e necessários à manutenção da disponibilidade das operações precisam ser efectuados. As organizações devem, então, dispor de planeamento e de mecanismos adequados à pronta recuperação de suas operações, no menor tempo possível, como forma de se precaverem dos efeitos desastrosos de eventos que causem interrupções significativas em parte, ou mesmo, em todos os seus processos de negócio.

O desenvolvimento de um plano de continuidade visa suprir uma necessidade da organização e decorre de uma decisão da administração. Envolve o compromisso de diversos intervenientes no processo de decisão e de execução, ou seja, de todos os recursos humanos envolvidos nos diversos processos organizacionais. A gestão da continuidade é, neste sentido, a ciência ou a arte de, reconhecendo a existência de ameaças, determinar as suas consequências nos recursos, aplicar alterações nos factores numa relação custo - benefício de forma a limitar as consequências.

Neste contexto, a sustentabilidade do negócio garantida por políticas de gestão da continuidade de negócio são um elemento central de boa governança das organizações em geral e das de cuidados de saúde em particular. Nesse desiderato, tem particular incidência a identificação dos riscos a que está sujeita a organização, a análise do impacto no negócio emergente e elaboração e manutenção de planos de continuidade que permitam, a minimização do risco inerente.

Afinal, bem vistas as coisas, não chovia quando Noé começou a construir a sua arca!

### **1.1 Motivação do estudo**

No contexto actual da sociedade, não basta a percepção do risco, antes importa que, através de um bom planeamento, estejam previstas as acções que minimizem o impacto das alterações planeadas ou não planeadas. A detecção e reconhecimento dos riscos inerentes, permitirão que os resultados ou consequências de alterações nos sistemas e processos das organizações sejam menos catastróficos.

Muitas organizações subestimam a importância destes planos por diversas razões: custos financeiros, falta de recursos qualificados, optimismo exacerbado, falta de cultura de planeamento e insuficiente sistema de gestão do risco. Por outro lado, as soluções existentes no mercado da consultoria especializada são de tal forma onerosas que, numa estrutura empresarial assente em micro, pequenas e médias empresas, constituem factor de reserva na tomada de decisão. Pensando no exemplo recorrente do atentado às torres do *World Trade Center* em Nova Iorque, no dia seguinte, milhares de funcionários não tinham onde ir trabalhar e dezenas de empresas ficaram sem os seus sistemas e dados mais importantes. Excepção desta trágica consequência daqueles que investiram na continuidade dos seus negócios, como o *Deutsch Bank* (Pritchard 2003, citado por (Erllich 2004)) que pode restabelecer as suas operações em pouco tempo.

A prestação de cuidados de saúde, independentemente da criticidade do acto clínico, tem um impacto essencial na vida dos cidadãos, pelo que factores como a avaliação do risco inerente e o desenvolvimento de planos de continuidade são cruciais para a manutenção desses cuidados.

A utilização das tecnologias de informação e de comunicação é crucial na prestação dos cuidados de saúde, fazendo com que aspectos como a disponibilidade dos sistemas, o armazenamento da informação, a sua recuperação em caso de falha e os modelos de decisão associados à gestão do risco reflectam a relevância dos mesmos nos planos de continuidade e de recuperação em caso de desastre.

As organizações devem desenvolver planos para as interrupções da actividade, definidas pelo Business Continuity Institute como "*any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at*

*an organization's location*". A gestão do inesperado é, assim, um dos maiores desafios com que as empresas têm de lidar, mas a dificuldade de antecipar acontecimentos inesperados torna esta responsabilidade nas organizações hospitalares especialmente desafiadora.

O risco está associado à possibilidade de perda de algo ou da probabilidade de ocorrência dessa perda, em razão de consequências externas ou internas. As componentes do risco, podem dividir-se em quatro: ameaças, recursos, alteração de factores e consequências.

A continuidade dos negócios, que num primeiro momento parece algo lógico e necessário a qualquer empresa, é domínio relativamente novo no sector da gestão de riscos corporativos. Todos os dias diversos sistemas sofrem interrupções, pessoas são vítimas de vírus, dados são obtidos ilegalmente e muitas empresas ficam, subitamente, sem poder laborar normalmente devido à falta de energia eléctrica.

## **1.2 Objectivo do estudo**

O objectivo deste estudo é, em primeira instância, estabelecer o retrato actual da implementação de políticas de gestão da continuidade do negócio, nas diversas componentes, no contexto hospitalar em Portugal, independentemente da personalidade jurídica e perceber as motivações destas organizações nesse desiderato.

Concomitantemente, há o propósito de desenvolver algumas das fases iniciais do processo de desenvolvimento de um plano de continuidade do negócio numa instituição de saúde. Por razões de limitação temporal do projecto, não é factível a demonstração de todas as fases que compõe o desenvolvimento do plano enumeradas e descritas nos capítulos subsequentes deste estudo.

As questões de investigação deste estudo procuram dar resposta às seguintes perguntas:

1. Qual o grau de maturidade dos sistemas de informação dos hospitais em Portugal?
2. Qual a importância que as organizações hospitalares em Portugal dão à existência de uma política de gestão da continuidade do negócio?
3. Existe, está implementado ou qual o grau de implementação da gestão da continuidade do negócio e dos elementos que a compõe?
4. Que tipo de constrangimentos existem para a implementação de um plano de continuidade do negócio?
5. Quais as principais dificuldades na implementação de um processo interno de gestão de continuidade?

## **1.3 Delimitação do estudo**

Este estudo procura identificar os diferentes graus de desenvolvimento de uma política de gestão da continuidade de negócio nos diversos hospitais portugueses e relatar as principais limitações na implementação dessa política.

O período escolhido para o inquérito foi limitado aos meses de Abril a Junho de 2010, tendo o estudo sido realizado em cerca de 100 hospitais públicos, privados e do sistema social a quem foi solicitado o preenchimento do questionário apresentado no capítulo 3.

Concernente à metodologia para o desenvolvimento de um plano de continuidade, o estudo desenrolou-se entre Março e Junho de 2010, no Hospital da Prelada Dr. Domingos Braga da Cruz, no Porto, uma instituição do sistema social de prestação de cuidados de saúde, onde foram efectuadas entrevistas directas e promovidos alguns procedimentos de identificação dos processos de negócio e da análise de impacto no negócio em caso de falha dos sistemas de informação.

#### **1.4 Estrutura do estudo**

Este relatório está organizado de acordo com as regras definidas pelo “Regulamento do Projecto ou Dissertação do MESG – Mestrado em Engenharia de Serviços e Gestão”, seguindo a estrutura tradicional de uma dissertação.

O capítulo 2 fornece o enquadramento teórico do papel dos sistemas de informação nas organizações, a problemática do risco e a temática da gestão da continuidade do negócio, seja numa perspectiva conceptual e holística, seja no desenvolvimento de cada um dos seus componentes – plano de emergência, plano de recuperação de desastres e plano de continuidade do negócio.

No capítulo 3 descreve-se a metodologia seguida na construção do questionário nacional sobre a gestão da continuidade do negócio nos hospitais portugueses, o universo e amostra de dados recolhidos e o seu grau de significância, o processo de recolha e tratamento dos dados e as limitações decorrentes da aplicação deste método.

O capítulo 4 apresenta a análise dos dados de cada um dos componentes do questionário e as inferências que dão resposta às quatro primeiras questões de investigação subjacentes a este estudo, a partir dos conceitos e teorias apresentadas na revisão da literatura.

No capítulo 5 é descrita a metodologia aplicada no desenho e desenvolvimento do Plano de Continuidade do Hospital da Prelada, desde o levantamento dos processos de negócio, o seu mapeamento com os sistemas de informação e identificação dos intervenientes em cada fase. É apresentado o método aplicado na licitação dos principais riscos inerentes, fazendo uso de metodologias de abordagem criativa e através da promoção de sessões de *role play* com os principais intervenientes nos processos.

Em anexos são apresentados os documentos utilizados em cada uma das fases deste estudo, desde o inquérito, ao desenvolvimento do caso de estudo.

## 2 Enquadramento Teórico

Desenvolveu-se um trabalho de revisão da literatura procurando conhecer as reflexões mais recentes sobre o tema, de forma a construir a estrutura teórica do estudo. Para tal recorreu-se a artigos científicos e, com particular destaque, a literatura especializada sobre a temática, produzida, nomeadamente, sob a égide de institutos de normalização e de boas práticas. De referir que este assunto não tem merecido atenção pela ciência em Portugal, na perspectiva holística que se apresenta, encontrando-se, no entanto, alguma produção científica em teses de mestrado e doutoramento circunscritas à problemática da segurança da informação, nomeadamente numa perspectiva tecnológica.

A revisão da literatura está estruturada em três subcapítulos. Em primeiro lugar perceber o impacto da informação nas organizações transformando-as estruturalmente em “organizações baseadas na informação”, utilizando o conceito de Drucker. Em segundo lugar analisar o papel do “risco” nas organizações. Na perspectiva da Gestão da Continuidade do Negócio (*BCM – Business Continuity Management*) o “risco” é a equação mais complexa que importa resolver, analisando as suas diversas incógnitas. Finalmente fazemos uma incursão teórica na temática da *BCM* de acordo com a perspectiva holística que se defende, da problemática da *BCM* como elemento aglutinador da estratégia de sustentabilidade da organização, sob o qual se desenvolvem os planos concretos que cumprem tal desiderato: plano de emergência, plano de recuperação de desastre e plano de continuidade do negócio. A organização temática deste subcapítulo serviu de base à construção do questionário, que será objecto de análise no capítulo seguinte, e ao desenvolvimento do caso de estudo no hospital, cujos resultados se apresentam no capítulo 5.

### 2.1 As Organizações baseadas na Informação

As organizações estão cada vez mais estruturadas em modelos organizacionais fundados no conceito de Drucker de “organização baseada na informação” (1998), com configurações estruturais horizontalizadas, permitindo uma melhoria no fluxo de informação. Estes modelos para além da melhoria da distribuição e aplicação da informação, propiciam a exploração dos conhecimentos existentes na organização e na sua envolvente, ao contrário dos modelos tradicionais que colocam a ênfase no processo de armazenamento da informação e na optimização da sua gestão operacional criada pelo desenvolvimento diário da organização (Serrano and Jardim 2007).

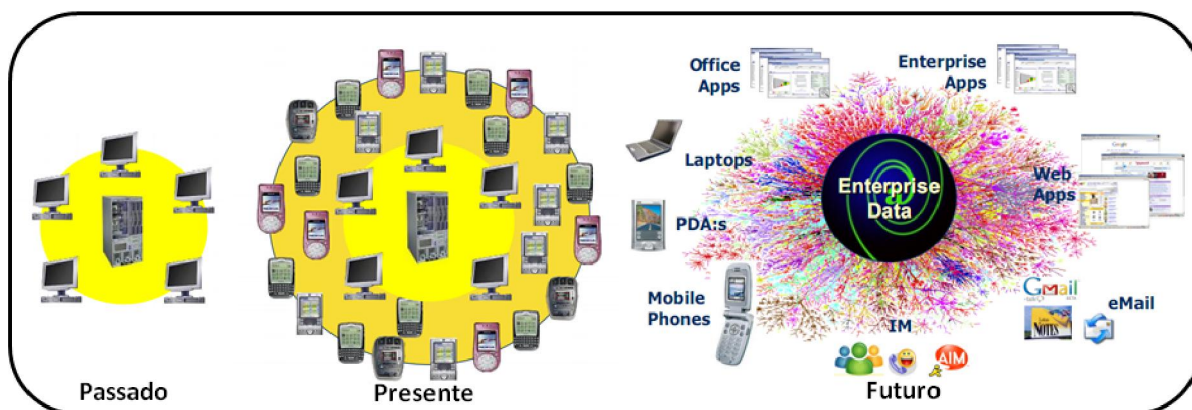
No actual estágio de desenvolvimento, confirmam-se os pressupostos apontados por Peter Drucker, há uma década atrás, sobre a “Nova Organização” (1998):

1. Necessidade de **informação disponível** para dar resposta à decisão de investimento;
2. Capacidade de **processamento de grande volume de informação** produzida na estrutura organizacional;
3. A introdução do conceito de **processo** como elemento nuclear do negócio, enquanto repositório de um conjunto de actividades, levadas a cabo por diferentes actores, com diversas competências e que transformam um conjunto de *inputs* em *outputs* que satisfaçam as necessidades dos seus *stakeholders*.

As organizações são mais complexas, com as tecnologias de informação a impactarem profundamente os seus sistemas de informação. Aos processos de negócio exige-se flexibilidade na reorganização dos seus componentes, que convirjam e integrem os novos elementos tecnológicos que vão surgindo e tornando obsoletos anteriores processos (Serrano and Jardim 2007). Novas formas de cooperação foram estabelecidas em resultado do desenvolvimento tecnológico e da evolução dos modelos organizacionais. As organizações necessitam de se envolver em “associações e consórcios estratégicos” que alarguem o âmbito da sua oferta e estendam a cadeia de valor da sua proposta. Outras empresas, escolas e universidades, entidades das administrações públicas, constituem os nós desta rede que partilha e integra diferentes competências e experiências.

Novas formas de trabalho, como o trabalho à distância, e o desaparecimento dos processos mecanizados, decorrem da massiva utilização das tecnologias de informação e comunicação nos processos das organizações. O contínuo “achatamento” das estruturas organizacionais, o fim da departamentalização burocrática e o surgimento das equipas de projecto, envolvendo diferentes competências, são faces deste movimento da “organização baseada na informação”.

Um dos indicadores deste movimento é a evolução das estruturas de rede nas organizações (Figura 1). Conceitos como *Cloud Computing*, *Software as Service*, *Virtualization*, *IT Leasing*, *Capacity on Demand*, *IT Outsourcing* e *Managed Services* integram e consubstanciam muitas das soluções dos sistemas de informação das organizações. A dependência tecnológica das organizações já há muito ultrapassou a fronteira geográfica da organização e do território onde está sediada e alargou o seu âmbito de acção a uma multiplicidade de canais de comunicação.



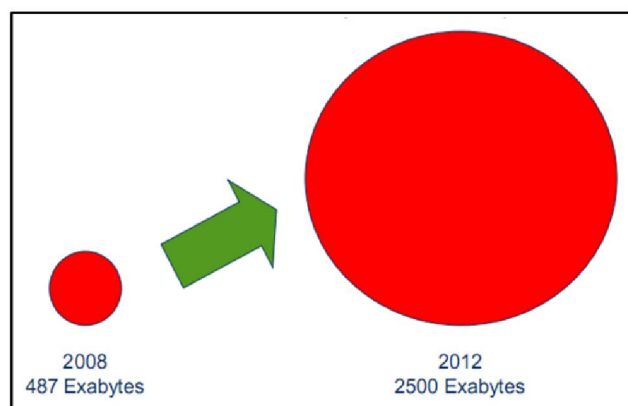
Adaptado de (Domage 2010)

Figura 1 - Evolução das estruturas de redes.

Um sistema de informação é um sistema complexo e necessita de uma abordagem multidisciplinar. Disciplinas como Ciências de Computadores, Operações e Gestão constituem a abordagem técnica dos sistemas de informação de gestão e que se complementam com a abordagem comportamental trazida pelas disciplinas da Sociologia, Psicologia e Economia, transformando os sistemas de informação em sistemas sócio – técnicos (Laudon and Laudon 2009). Outro elemento que caracteriza a evolução da informação digital nas organizações é o seu volume. A Figura 2 representa o crescimento do volume de informação criada, capturada e replicada pelos sistemas de informação. A tendência é que no espaço de cinco anos o volume de informação quintuple.

Novos desafios tecnológicos são colocados às organizações para preservar e disponibilizar, em tempo útil, a informação necessária e resultante dos seus processos de negócio. Soluções como a *Deduplication*, *Virtualization*, *Storage as a Service*, *Cloud Storage* são propostas tecnológicas na resposta a esta necessidade.

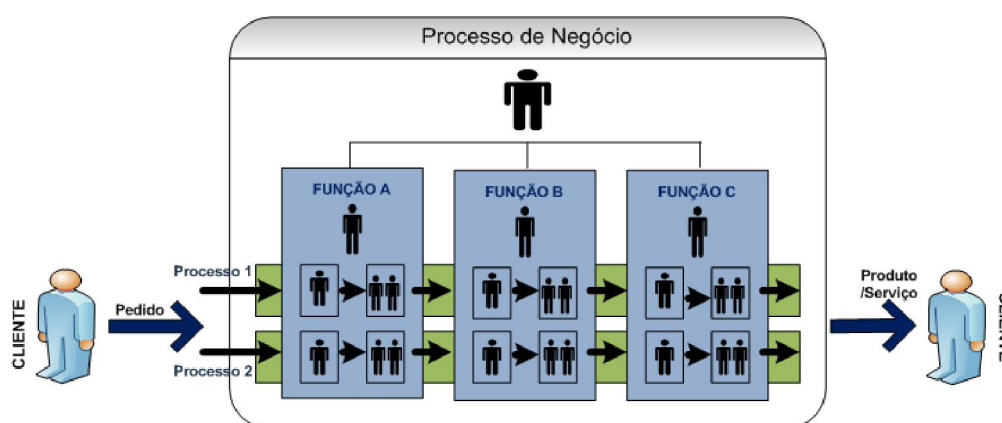
Neste contexto de alteração do paradigma das estruturas organizacionais impactadas pelas Tecnologias de Informação e Comunicação (TIC) e pela dependência das organizações pela informação, uma política de gestão da continuidade assume toda a importância e acuidade. Não é imaginável que uma organização corra riscos pela indisponibilidade da informação e dos seus sistemas.



Adaptado de (Domage 2010)

Figura 2 - Informação Criada, Capturada e Replicada.

A importância do fluxo da informação nas organizações decorre do desenvolvimento de novas abordagens nos modelos de negócio. As organizações funcionam em pequenos ciclos de tempo, aumentando a pressão para diminuir os custos e aumentar a eficiência, orientando a sua actividade para a satisfação do cliente (Vancoppenolle 2007). Hoje as organizações estão organizadas sobre processos de negócio (Figura 3). Para entregar um produto ou serviço a um cliente, um conjunto de actividades são executadas. Este conjunto de actividades denomina-se por “processo de negócio”. Muitas organizações ainda persistem numa organização assente em divisões e departamentos, seguindo uma orientação hierárquica formal, em que as diversas actividades são organizadas e executadas pelos diversos departamentos, através de processos de negócio que exigem fluxos de informação.



Adaptado de (Vancoppenolle 2007)

Figura 3- O Processo de Negócio.

Uma organização estruturada através de processos de negócio, é uma organização integrada, numa perspectiva tridimensional, em que Processos, Pessoas e Infra-estrutura e Recursos participam na missão da organização, sendo a informação a malha que interliga integralmente a todas as dimensões da organização (Figura 4).

Nesta perspectiva, cada elemento pode ser caracterizado por:

- **Processos:** como os produtos e serviços são entregues aos clientes;
- **Pessoas ou Participantes:** Quem participa na execução dos processos de negócio;
- **Infra-estrutura e recursos:** O que é utilizado na execução dos processos de negócio;

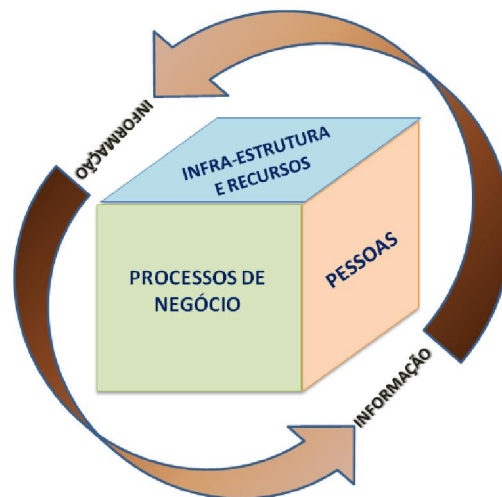


Figura 4 - Elementos da Organização Integrada

Cada processo depende de um conjunto de elementos críticos. As pessoas são participantes críticos no processo, com as suas competências e conhecimento, pelo que constituem uma das dependências do processo. Por outro lado, as pessoas não inseridas em processos tornam-se elementos que não contribuem para a missão da organização, antes afectam negativamente a sua eficiência. As outras dependências são a infra-estrutura da organização e os recursos. Está-se a falar de recursos de logística, infra-estruturas administrativas, industriais e tecnológicas ou recursos financeiros. A infra-estrutura e os recursos alocados devem estar alinhados com os processos e seus participantes, com a flexibilidade e adaptabilidade que permitam uma eficiente e eficaz utilização. Nesta relação tridimensional de interdependência, o fluxo de informação é crítico para o alcançar do desempenho e a eficiência da organização. A falta da informação, devido a um evento, interrompe toda esta rede de dependências e impacta negativamente as operações do negócio, podendo afectar com elevadas consequências toda a organização.

No entanto, a organização para cumprir a sua missão está dependente de recursos que lhe são externos e de outras organizações, sob pena de se transformar numa ilha. Esta dependência externa traz aos processos de negócio uma perspectiva de “*extended enterprise*” (Vancoppenolle 2007) Este conceito foi utilizado pela primeira vez na *Chrysler Corporation* associado à troca de informações para redução de custos na cadeia de abastecimento (Post, Preston, and Sachs 2002). Na perspectiva de Post, Preston et al., o conceito de “*extended enterprise*” foi alargado, de forma a incluir, para além das interacções da organização com

outros parceiros do negócio, as relações com todos os *stakeholders*, sejam externos ou internos. A “*extended enterprise*” é um elemento nodal de uma rede de *stakeholders* interrelacionados que criam, sustentam e aumentam a sua capacidade de co-criação de valor.(Post, Preston, and Sachs 2002) A capacidade da organização ser bem sucedida e sobreviver no longo prazo depende da sua capacidade em estabelecer e manter relacionamentos dentro desta rede de *stakeholders*.

### **2.1.1 Os Sistemas de Informação hospitalar**

A introdução das TIC nos sistemas de informação hospitalar (*HIS – Health Information Systems*) tem crescido exponencialmente. A sua presença no quotidiano da actividade hospitalar é inequívoca, seja no suporte aos processos administrativos, seja no suporte ao acto médico, desde o diagnóstico até à prescrição, passando pelo tratamento. Os dados reportados em cada um dos sistemas permitem identificar os doentes, as patologias, os tratamentos e, por vezes, os seus hábitos (Katsikas 2000).

Outra alteração substancial nos *HIS* foi a passagem de um sistema baseado em equipamentos *stand-alone* para soluções em rede, quer interna, quer externa, criando uma vasta e complexa comunidade em rede. O aumento do uso de redes locais (*LAN – Local Area Network*) e redes globais (*WAN – Wide Area Networks*) para além de criar enormes possibilidades, também trouxe novas vulnerabilidades e o aumento de falhas de segurança e pontos de falha nos sistemas de informação (Katsikas 2000). A evolução dos *HIS* impactou os contextos sociológicos dos hospitais alterando a rotina dos seus colaboradores, bem assim como os diversos papéis em presença, nomeadamente por parte dos clínicos que foram chamados a acções que, em regra, não lhes estavam cometidas como a actualização dos processos clínicos electrónicos.

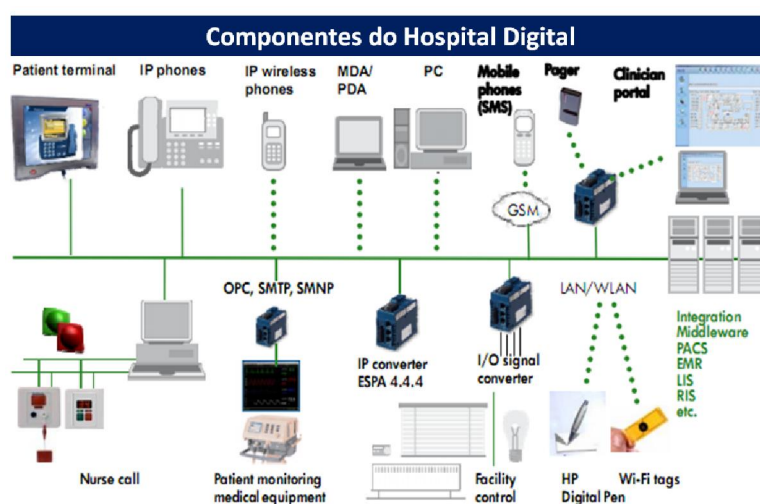
Para Shortliffe and Cimino (2006), um sistema computacional de incidência hospitalar deverá conter as seguintes oito funções:

1. Recolha de dados e Apresentação;
2. Protecção dos Dados e do Acesso;
3. Comunicação e Integração da Informação;
4. Segurança;
5. Salvaguarda e Recuperação da Informação;
6. Análise de Dados;
7. Suporte à Decisão;
8. Educação;

Com o desenvolvimento dos *HIS*, o conceito de Hospital Digital assume particular relevância, como abordagem conceptual para a entrega de serviços de saúde que incorpora um design multi-disciplinar e uma abordagem baseada na teoria dos sistemas. A teoria dos sistemas é um enquadramento para a análise e descrição de objectos que trabalham conjuntamente para produzir um desejado resultado, que neste caso, visam otimizar a entrega de serviços de saúde, considerando as inter-relações entre as instalações, equipamentos, pessoal, pacientes, processos e tecnologia (Shortliffe and Cimino 2006). Na concepção deste hospital do futuro, informação e TIC desempenham um importante e penetrante papel em assegurar a eficiência e a qualidade dos cuidados prestados (Ginzberg 1996).

Um hospital digital é aquele que:

- Tem implementado uma abrangente e penetrante infra-estrutura de TI que permite o *workflow* do trabalho clínico e administrativo, gestão de processos e melhorias na qualidade;
- Iniciou um processo de expansão das melhorias no hospital para além das quatro paredes, permitindo a conectividade e colaboração com consultórios médicos e outras organizações de saúde, até alargar o seu alcance digital aos lares dos pacientes, serviços de emergência e outros serviços médicos;
- Utiliza várias tecnologias avançadas, como dispositivos médicos cruciais, sistemas de informação inteligente, sistemas de controlo automatizado, sistemas de transporte, sensores e instrumentos de comunicação digital, proporcionam um conjunto integrado de aplicações e serviços que melhoram a produtividade dos funcionários, as operações do hospital, a qualidade do processo e a segurança do paciente.



Fonte: HP, 2009

Figura 5 - Componentes do Hospital Digital

O papel das TIC nos *HIS* pode comparar-se ao de um sistema circulatório, num ecossistema de cuidados de saúde. De acordo com o Modelo de Maturidade dos Sistemas de Informação dos Cuidados de Saúde desenvolvido pela IDC Health Insights (2008), existem cinco estágios de desenvolvimento, em função da capacidade dos *HIS*:

- ***HIS Básico***: Está implementado o núcleo dos sistemas financeiros e administrativos para dar suporte ao registo do paciente, facturação do paciente e contas a receber, recursos humanos e finanças em geral, e outras funções de negócios de *back-office*.
- ***HIS Avançado***: Além das aplicações básicas, este estágio oferece mais capacidades administrativas, tais como apresentação créditos electrónicos e processamento de pagamentos.
- ***HIS/CIS Avançado***: Os hospitais começam a lançar as bases para registos médicos electrónicos (*EMRs*) através da implementação dos sistemas de informação clínica (*CIS*), incluindo sistemas de informação do laboratório (*LIS*), sistemas de informação de radiologia (*RIS*) / apresentação dos resultados de radiologia, arquivamento de imagens e de comunicação com sistemas (*PACS*), e farmácia.
- ***Hospital Digital***: Uma vez implementado o núcleo dos sistemas de informação clínica, os hospitais começam a implementar a infra-estrutura necessária para suportar mais aplicações clínicas avançadas, tais como a tecnologia *Computerized Physician Order Entry* CPOE (CPOE), actualização de documentação clínica por *wireless*, uso

de tecnologia de portal Web pelos pacientes e funcionários, e um prontuário electrónico completamente funcional.

- **Corporação Digital Virtual:** Os hospitais mais avançados não só têm totalmente automatizado os seus negócios e funções clínicas, como também têm um robusto repositório de dados clínicos (CDR), complementado por ferramentas de *report* de informação clínica, estão a estender o alcance clínico para além da instituição usando a telemedicina e monitorização remoto de pacientes e a participação em iniciativas regionais de intercâmbio de informações.

## 2.2 O Risco nas Organizações

Definir “risco” é uma tarefa inglória. Na década de 90, a *Society for Risk Analysis*, organizou um comité de especialistas com o propósito de construírem uma definição de “risco”. Após quatro anos de laboriosa actividade, acabaram por desistir e declaram que o melhor seria não definir o significado de “risco” e deixar cada autor apresentar a sua própria definição (Kaplan 1997).

Não se tem a pretensão de contribuir para uma definição “original” ou de contrariar o conselho dos “sábios”. Socorre-se da definição de Vose (2000) que define “risco” como:

- Um evento aleatório com possibilidade de ocorrência e que, se ocorrer, terá um **impacto negativo** nos objectivos da organização. Assim, o “risco” é composto por três elementos:
  1. O cenário;
  2. A probabilidade de ocorrência;
  3. A dimensão do impacto, no caso de ocorrência;

Por contraponto, Vose define a “oportunidade” também como um evento aleatório com possibilidades de ocorrência, mas com um **impacto positivo** nos objectivos da organização. Também a “oportunidade” é composta pelos mesmos três elementos. Nesta definição, “risco” e “oportunidade” são faces da mesma moeda (Vose 2000). O factor chave desta definição está na qualidade do impacto gerado pelo evento.

Para Kaplan (1997) definir “risco” é responder a três questões:

1. O que pode acontecer?
2. Qual a probabilidade de isso acontecer?
3. Se acontecer, quais serão as consequências?

A resposta à primeira questão conduz à elaboração do “cenário”, a segunda dá a probabilidade da ocorrência de cada “cenário” e a terceira o impacto desse “cenário”. Da composição das três respostas, Kaplan propõe uma fórmula de quantificação do risco através da equação

$$= \{ \quad , \quad ( \quad ) , \quad ( \quad ) \} ,$$

em que

- $\quad$  representa os diversos cenários,
- $( \quad )$  a probabilidade de ocorrência de cada um dos cenários e
- $( \quad )$  o impacto de cada cenário (Kaplan 1997).

A proposta de Kaplan conduz a uma análise do tipo “*what if*” com a construção de múltiplos cenários e respectiva quantificação do impacto.

Para além da cenarização, determinação probabilística e mensuração dos impactos, a análise de risco é importante para a categorização do risco, devendo utilizar uma lista de categorias que auxiliem a identificação.

O’Hehir (2007) divide os riscos em cinco grupos nucleares e que podem ser úteis como ponto de partida na análise do risco:

- v **Estratégicos:** o risco dos planos falharem por;
  - o Estratégia de marketing mal definida;
  - o Estratégia de aquisições errada;
  - o Alterações no comportamento dos consumidores;
  - o Alterações políticas ou legislativas;
  - o ...
- v **Financeiros:** o risco dos controlos financeiros falharem por:
  - o Riscos de tesouraria;
  - o Falta de contrapartidas ou má avaliação do crédito;
  - o Fraudes sofisticadas;
  - o Falha dos sistemas;
  - o Stocks mal definidos;
  - o ...
- v **Operacionais:** o risco de erro humano por:
  - o Erros no desenho;
  - o Práticas de risco;
  - o Comportamentos não seguros;
  - o Sabotagem;
  - o ...
- v **Comerciais:** o risco de as relações comerciais falharem por:
  - o Falta de um executivo principal;
  - o Falhas no fornecimento;
  - o Falhas na conformidade dos produtos/serviços;
  - o ...
- v **Técnicos:** o risco de activos físicos falharem ou ficarem danificados por:
  - o Quebra no funcionamento dos equipamentos;
  - o Falha na infra-estrutura;
  - o Incêndio;
  - o Explosão;
  - o Poluição;
  - o Seca ou outros riscos naturais;
  - o ...

Estes grupos de risco não são mutuamente exclusivos, antes devem merecer uma abordagem integrada. A resposta ao risco é diversa. A literatura apresenta as opções que a direcção das organizações pode escolher face aos riscos e que Vose (2000) sistematiza:

1. **Aceitação** – não fazer nada! Sempre que o custo do controlo do risco é incomportável para a organização e a probabilidade de ocorrência é baixa. Seguindo esta opção deverá ser elaborado o Plano de Contingência apropriado.

2. **Aumento.** Se da análise decorrer a convicção de que estão alocados recursos exagerados na gestão do risco comparado com o nível de protecção que garantem, deve ser reduzido o nível de protecção e alocado a outros recursos.
3. **Obter mais informação.** Havendo incerteza que dificulte a tomada de decisão, a opção pode ser a de obter mais informação que habilite o analista a construir a análise de risco.
4. **Eliminação.** Esta opção envolve a alteração do método da operação, um novo projecto, uma estratégia de investimento, etc., de forma que identificar o risco se torna irrelevante. A eliminação em regra envolve riscos com elevada probabilidade ou grande impacto.
5. **Redução ou mitigação.** Esta opção envolve a utilização de um conjunto de técnicas que, utilizadas conjuntamente, reduzem a probabilidade do risco e do seu impacto. Exemplo disto são soluções de:
  - a. Redundância (Equipamentos de substituição, *backups* noutras localizações)
  - b. Execução de testes e inspecções mais frequentemente;
  - c. Melhor formação dos colaboradores;
  - d. Propagar o risco por diversas áreas;
6. **Plano de Emergência:** Existência de planos desenvolvidos que optimizem a resposta ao risco em caso de ocorrência. O plano deve identificar o que fazer, como fazer, quem o deve fazer e em que ordem, a janela de oportunidade, etc.

No portfólio de riscos associados às TIC, com um negativo impacto no negócio, destacam-se as seguintes áreas:

- Projectos: falhas nas entregas;
- Continuidade dos serviços de TIC: falhas na prestação do serviço ou interrupção;
- Activos de Informação: não protegidos ou preservados;
- Prestadores de serviços ou *vendors*; falhas nas entregas;
- Aplicações: falhas nos sistemas;
- Infra-estrutura: mau dimensionamento; (Jordan 2005)

De acordo com o *Strategic Research Group* ([www.strategicresearchgroup.com](http://www.strategicresearchgroup.com)) as causas principais de falhas nos Sistemas de Informação com impacto na continuidade do negócio devem-se a:

- 44% Hardware - Falhas nos componentes (inclui servidores, switches, discos rígidos, controladoras RAID e outras peças nucleares da infra-estrutura) causando quebra no serviço e/ou nos níveis de serviço;
- 32% Erros humanos - Configuração dos sistemas ou instruções erradas na administração e operação dos sistemas.
- 14% Erros de Software e Firmware - Estrangulamento nos sistemas, incompatibilidades nos *drivers* e a introdução de novas aplicações nos servidores exigem mais recursos que os disponíveis;
- 7% Vírus/Brechas de Segurança - Preemência de ataques malévolos ou da descarga de ficheiros infestados.
- 3% Desastres Naturais.

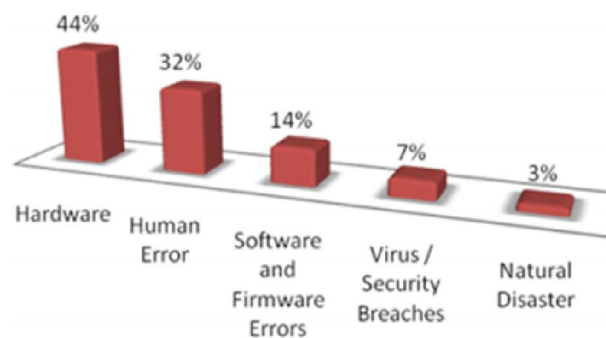
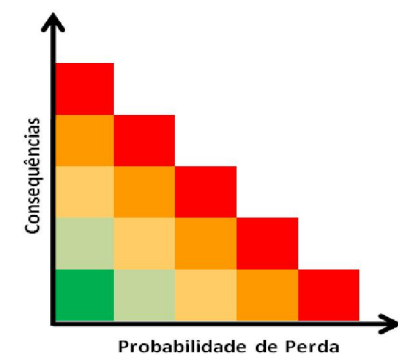


Figura 6 - Eventos disruptivos dos SI

Existem diversas abordagens na gestão do risco. Socorremos da abordagem de Jordan, de, a partir da identificação dos processos de negócio, analisar a vulnerabilidade de cada um deles (2005). A vulnerabilidade dos processos é resumida numa matriz de vulnerabilidade (Figura 7) onde é identificada a relação entre a probabilidade de perda e a respectiva consequência. Esta abordagem conduz à Análise de Impacto no Negócio (*BIA – Business Impact Analysis*), um elemento central do Plano de Continuidade do Negócio (*BCP – Business Continuity Planning*), que se descreve no próximo subcapítulo.



Adaptado de (Jordan 2005)

Figura 7 - Matriz de Vulnerabilidade.

No contexto hospitalar, uma característica que qualquer profissional do sector tem bem presente no exercício da actividade é a percepção do risco. Desde o risco de vida dos seus utentes, os riscos infecciosos, os riscos associados ao uso de tecnologias complexas e todos os demais riscos a que as organizações em geral estão sujeitas. Por razões óbvias, a percepção do risco e a forma como as organizações hospitalares desenvolvem estratégias de salvaguarda e minimização constitui um elemento central da boa governança e da importância que atribui à *BCM*.

### 2.3 Gestão da Continuidade do Negócio

Num ambiente de permanentes ameaças, a *BCM* afirma-se como um processo sistemático para combater o efeito das crises e das interrupções da prestação de serviço (Herbane, Elliott, and Swartz 2004). O *Business Continuity Institute* define a *BCM* como “um processo holístico de gestão que identifica potenciais impactos que ameaçam a organização e fornece um enquadramento para a construção de resiliência e da capacidade para uma resposta efectiva

que proteja os interesses dos *stakeholders*, a reputação, a marca e as actividades criadoras de valor”<sup>1</sup> (BS25999-2) Nesta perspectiva, a *BCM* está associada aos processos que identificam a exposição da organização a ameaças interna e externas, os activos de hardware e software com vista ao estabelecimento de um plano de prevenção e recuperação. Para Vancoppenolle, a *BCM* consiste na capacidade de continuar “*without missing a beat*” ou estar preparado para reconstruir a organização após um desastre, de forma a garantir a continuidade da prestação do serviço a um nível minimamente aceitável, limitando o impacto financeiro e permitindo a sobrevivência da organização a longo prazo (2007).

Os efeitos resultantes do ataque terrorista às torres do *World Trade Center* demonstraram que algumas empresas estavam dotadas de instrumentos que lhes permitiram recuperar, num curto espaço de tempo face ao impacto do incidente, Para além do exemplo do *Deutsch Bank* já referido, há o caso do *Morgan Stanley*, outra instituição do universo financeiro. A abordagem desenvolvida pela empresa assentava não somente na estratégia de *disaster recovery* dos sistemas informáticos, mas envolvia uma filosofia da organização que foi demonstrada na adaptação organizacional, antes e depois do colapso. Esta estratégia permitiu-lhes evidenciarem-se não somente na recuperação dos dados existentes nos sistemas, como conseguiu que a maioria dos 3.700 funcionários sobrevivesse ao colapso da torre sul, muito graças ao processo formativo que os funcionários tinham recebido. Três dias após o desastre todos os seus funcionários tinham sido localizados e um centro alternativo estava disponível e operacional noutra zona da cidade (G. Silverman and P. T. Larsen 2001) *quoted in* (Herbane, Elliott, and Swartz 2004).

As recentes catástrofes naturais, como é o caso do vulcão Eyjafjallajökull, provam a imprevisibilidade dos acontecimentos. Se a isto juntarmos os ataques terroristas, a degradação de equipamentos, os acidentes causados pelo homem, etc., levam as organizações a reconhecerem, mais do que nunca, a necessidade de estarem preparados para o imprevisto. A oferta contínua de serviços, 24x7, o desenvolvimento do comércio electrónico, traz exigências de disponibilidade às organizações, com reduzidos tempos de recuperação em caso de falha. Estas exigências manifestam-se nos seguintes elementos:

- Os clientes esperam que os fornecimentos de bens e serviços se mantenham ou que retomem em todas as situações;
- Os accionistas esperam que o controlo de gestão esteja operacional em qualquer situação de crise;
- Os funcionários esperam que os seus postos de trabalho estejam salvaguardados e que o seu estilo de vida se mantenha;
- Os fornecedores esperam manter as suas encomendas e os fluxos de receita associados;
- Os órgãos reguladores esperam que as suas exigências sejam cumpridas;
- As empresas de seguros esperam que a organização proteja e cuide convenientemente dos seus activos;

A *BCM* é hoje uma disciplina da gestão que tem ocupado o seu lugar em todos os sectores da actividade económica, bem assim como nos diversos níveis das administrações públicas em todo o mundo. A necessidade de uma abordagem integrada é cada vez mais o paradigma da

---

<sup>1</sup> Tradução livre do autor.

*BCM*. Todos os níveis da actividade, incluindo as diversas administrações públicas, necessitam de um processo de *BCM* e este deve ser coordenado por uma equipa de gestão centralizada que garanta a consistência, integração, economias de escala e a eficiência em geral (Hiles 2007). Não há lugar no processo da *BCM* a uma abordagem do tipo “silo”. Ao contrário, no contexto organizacional a *BCM* é um processo que identifica a exposição da organização a ameaças internas e externas e assegura os recursos *hard* e *soft* que permitam uma efectiva prevenção e recuperação. O essencial para assegurar o sucesso da *BCM* está na completa compreensão da ampla gama de ameaças (internas e externas) e o reconhecimento que uma eficaz resposta dependerá do comportamento das pessoas envolvidas durante o processo de recuperação do negócio, desde os especialistas até aos colaboradores da organização (Herbane, Elliott, and Swartz 2004). Pessoas e processos são fundamentais e inseparáveis. A prioridade, em situação de crise, deve ser o acesso das pessoas habilitadas a recuperar o negócio, pois nada será recuperado ou restaurado.

No entanto não é possível estar preparado para todos os possíveis eventos. A maioria dos eventos de grande dimensão é rara e imprevisível. Daí a questão “Como podemos planear algo que não se conhece ou da qual desconhecemos a probabilidade?”

### 2.3.1 Dimensões da Gestão da Continuidade do Negócio

Como um processo holístico, a *BCM* representa-se em diferentes dimensões, interdependentes, que confluem no único propósito de dotar a organização de um processo que a habilite a vencer eventos que comprometam a sua missão: dimensão estratégica, dimensão operacional e dimensão humana.

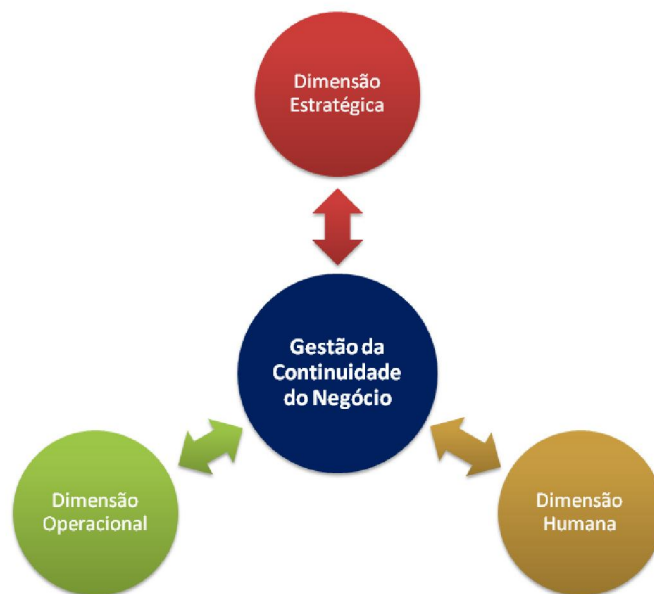


Figura 8 - Dimensões da Gestão de Continuidade do Negócio

## Dimensão Estratégica

A *BCM* é um processo organizacional estratégico pois visa garantir a “*survivability*”<sup>2</sup> da organização, a satisfação dos seus *stakeholders*. Esta estratégia persegue um conjunto de objectivos-chave: (Smith 2003)

- Garantir a segurança dos funcionários;
- Maximizar a defesa da reputação da organização e da sua imagem de marca;
- Minimizar o impacto dos eventos (desastres e crises) nos clientes;
- Limitar e prevenir o impacto para além da organização;
- Demonstrar uma governança efectiva e eficiente para os média, mercados e *stakeholders*;
- Proteger os activos da organização;
- Respeitar os requisitos legais, regulamentares e de segurança;

A *BCM* oferece à organização uma abordagem que lhe permite melhorar a *continuidade das operações* na circunstância de ocorrência de um desastre ou crise. Sem esta capacidade organizacional, a dimensão estratégica da vantagem competitiva poderá não ter uma plataforma segura que lhe permita gerar valor no futuro (Herbane, Elliott, and Swartz 2004). A continuidade operacional é uma **vantagem competitiva** da organização, permitindo-lhe isolar-se da concorrência e obter vantagens competitivas face aos riscos e vulnerabilidades conhecidas e que possam afectar a sua reputação, solvência e sobrevivência.

A continuidade operacional também contribui para **preservar o valor**. A capacidade da organização em resistir às crises e recuperar rapidamente, minimizando o impacto das perdas é identificada como preservação do valor (Herbane, Elliott, and Swartz 2004). A preservação do valor é uma capacidade intrínseca (que inclui recursos de continuidade de negócios, processos, rotinas e *know-how*) que é sustentada pela *BCM* e proporciona uma maior estabilidade. Não se sugere que a *BCM* conduz necessariamente a vantagem competitiva, mas sem a *BCM* a exposição ao risco da organização pode ser bem elevado.

Finalmente o papel estratégico da *BCM* assume nos processos de recuperação efectiva e de restauração das práticas organizacionais uma **vantagem de recuperação**, não só porque permite uma mais rápida recuperação das operações e actividades como combate as ameaças à reputação na fase pós-crise (Herbane, Elliott, and Swartz 2004).

O papel estratégico da *BCM* deve reflectir a complexidade do perfil de risco de uma organização, o ambiente em que se insere e deve unificar as várias disciplinas de gestão da organização. Muitas organizações concentram-se somente na vertente dos SI e acabam por deixar lacunas nas restantes funções da disciplina. Na perspectiva de Smith, a *BCM* é um processo que, tal como um guarda-chuva, protege todos os sectores da organização.

---

<sup>2</sup> A capacidade de um sistema para cumprir a sua missão, em tempo oportuno, na presença das ameaças tais como ataques ou desastres naturais em grande escala. A *survivability* é um subconjunto da resiliência (capacidade de resistir às adversidades).



Adaptado de (Smith 2003)

Figura 9 - Processo unificador.

Uma estratégia de continuidade de negócios é um valor cimeiro na organização. Ela envolve um amplo espectro de tecnologias: velhas e novas, baseadas em papel e em suporte electrónico, manual e automatizada, individual e integrada. No entanto, o maior desafio na construção de um processo de continuidade não é tecnológico, antes se circunscreve ao marketing empresarial interno (Noakes-Fry and Diamond 2001). A sua eficácia depende do envolvimento inquestionável da administração em todo o projecto, desde a concepção e implementação até à actualização e testes para a manutenção.

### Dimensão operacional

A organização que implementa processo de *BCM* alicerça esta iniciativa em dois objectivos: sobrevivência e resiliência.

A **sobrevivência** e a *BCM* são, como referimos, dois conceitos intimamente ligados. O *The American Heritage Dictionary of the English Language* descreve a *survivability* como a capacidade de resistir num ambiente hostil ou de suportar um ataque ou contra-medidas (*The American Heritage Dictionary of the English Language* 2006). De acordo com um relatório do *Gartner Group* somente 6% das empresas sobreviveu mais do que dois anos após perda de informação. Das empresas analisadas pela *Gartner*, 43% encerrou as portas imediatamente após a perda de dados, enquanto que 51% resistiram cerca de dois anos (HSNW 2010).

A sobrevivência é a capacidade de uma organização cumprir a sua missão, em tempo útil, na presença de ameaças como ataques ou desastres naturais. Nesta definição convergem duas concepções de ameaças: as ameaças que decorrem de um ataque inteligente de um adversário e as de grande porte devidas à infra-estrutura de suporte aos SI da organização (Sterbenz et al. 2010).

Para Quirchmayr é necessária uma abordagem mais abrangente para que a segurança dos SI sobreviva a intrusões bem sucedidas (2004). Desde os ataques de 11 de Setembro de 2001 a BCM e a sobrevivência constituem uma preocupação comum. O “cyber-terrorismo” e outras formas de ataque são encaradas com maior seriedade e isso tem implicações profundas na cultura organizacional. A sobrevivência exige uma diversidade de respostas, pois é improvável que a mesma resposta possa ser partilhada por partes de um sistema sujeito a falhas correlacionadas (Sterbenz et al. 2010). Tal decorre da multiplicidade de variáveis que concorrem para uma resposta.

A **resiliência** – capacidade da organização cumprir a sua missão, mesmo em condições adversas – é um factor de *stress* relacionado com a gestão operacional da organização, em grande medida motivado pela:

- Complexidade dos avanços tecnológicos que necessitam de suporte e recursos muito especializados, criando um ambiente repleto de vulnerabilidades e riscos;
- Necessidade de parcerias no desiderato da missão da organização. Os parceiros exteriores fornecem competências e funções fulcrais, que permitem à organização melhorar a sua eficiência, aumentando a produtividade e reduzindo os custos. Como resultado a organização expõe-se a novos riscos ao ceder o controlo a agentes exteriores como garantia do cumprimento da sua missão e redução dos custos;
- O mundo globalizado e a integração das cadeias de fornecimento em interdependências globalizadas são um problema de gestão da governança e controlo que está para além das fronteiras geográficas e organizacionais; (Caralli et al. 2010)

A resiliência operacional é uma propriedade que emerge da capacidade de uma organização prosseguir a sua missão após uma ocorrência disruptiva da sua actividade, que não exceda o seu limite operacional (Caralli et al. 2010).

Os factores descritos obrigam a organização a repensar como gere o risco e como trata a resiliência dos processos de negócio críticos.

A resposta tradicional, compartimentada, silo-funcional, não serve os novos desafios, nem responde às questões: Quão resistente é a organização a novos riscos e constrangimentos? É resistente o suficiente? A resposta baseada na avaliação de eventos passados, apesar de necessária, não fornece as garantias para novas ameaças, sendo fundamental a organização estar preparada para prever como irá responder a alterações do ambiente de risco. As respostas produzem-se em diversas dimensões da organização. Numa primeira fase, é necessário que as actividades de gestão da segurança, da continuidade do negócio e das operações de TI – actividades típicas na gestão do risco – convirjam para um *contínuo* de práticas focadas na resiliência operacional. Em segundo lugar, é necessária uma correcta e confiável avaliação da capacidade e que sirva de base à melhoria de processos. Finalmente, as respostas devem permitir a organização melhorar os processos deficientes, diminuindo as lacunas que se traduzem em fraquezas e afectam a resiliência operacional e a capacidade da organização atingir os objectivos estratégicos (Caralli et al. 2010).

## Dimensão humana

As organizações são compostas por pessoas e os seus dirigentes devem promover a liderança cultural. A *BCM* não é um conjunto de ferramentas, técnicas e mecanismos a ser implementados na organização. A *BCM* é um processo que deve reflectir uma atitude geral e um tipo de acção desenvolvida pela direcção da organização e pelos seus funcionários. Os indivíduos desempenham um papel crucial e crítico neste processo. Como refere Smith, a dimensão humana é frequentemente subavaliada na *BCM*, nomeadamente na avaliação das causas dos eventos de continuidade e nas crises. Estas sinalizam diversos avisos que são ignorados ou não reconhecidos (Smith 2003). No processo holístico que se apresenta, uma das primeiras tarefas é a identificação das pessoas que estão envolvidas com a cultura da organização. É uma das condições de sucesso de um processo de *BCM* o engajamento dessas pessoas com a estratégia de continuidade da organização.

A dimensão humana da *BCM* reflecte-se desde logo na condução de todo o processo. Pelo exposto se reconhece a exigência de que este processo esteja sob a liderança da alta direcção da organização. A liderança é uma das principais forças no processo de melhoria de desempenho de uma organização. Os líderes, como *decision-makers*, determinam a aquisição, desenvolvimento e implementação dos recursos e a conversão desses recursos em produtos e serviços de valor acrescentado e a entrega do valor aos *stakeholders* da organização. São necessários líderes que conduzam a organização a atingir os seus objectivos de forma eficiente e que desenvolvam uma visão estratégica que conduza a elevados níveis de coesão, compromisso, motivação e desempenho (Zhu, Chew, and Spangler 2005).

Por outro lado, as pessoas são o activo mais importante de uma organização e a sua capacitação é um dos factores críticos de sucesso para a sobrevivência das organizações nestes novos tempos. Nessa medida, torna-se necessário que neste processo sejam envolvidas pessoas pró-activas, com capacidade para agir e ousar, que procurem novas soluções e estejam motivadas nesse objectivo (Serrano and Jardim 2007). As organizações devem, em sede de *BCM*, recorrer a pessoas intimamente ligadas com a cultura da organização e com profundo conhecimento dos seus processos de negócio. O processo de recuperação em caso de desastre está muito para além da salvaguarda da informação e da sua disponibilidade. É fundamental que a *BCM* contemple as acções que incluam o restabelecimento do ambiente de trabalho e das condições psicossociais da organização.

### 2.3.2 Abordagens na implementação da Gestão da Continuidade do Negócio

A *BCM* é um processo estratégico na minimização do risco e na construção da sustentabilidade da organização. Enquanto processo holístico materializa-se através de diversos instrumentos (Figura 10), observada uma metodologia no seu desenvolvimento. Neste propósito, numa perspectiva global, a *BCM* persegue os seguintes objectivos:

- Minimizar o impacto do desastre numa organização – **Plano de Emergência** (*EP – Emergency Plan*);
- Desenvolver um plano de recuperação pragmático, operacional e com custo aceitável, que permita à organização manter os processos de negócio críticos na ocorrência de eventos que provoquem a disrupção das operações – **Plano de Recuperação de Desastres** (*DRP – Disaster Recovery Plan*);

- Desenvolver um enquadramento para a avaliação dos processos de negócio que permitem uma abordagem focalizada no desenvolvimento de um plano de continuidade através de uma metodologia bem estruturada e perceptível – **Plano de Continuidade do Negócio** (BCP – *Business Continuity Plan*);



Figura 10 - Componentes da Gestão de Continuidade do Negócio

A aplicação de um processo de *BCM* é uma vantagem competitiva para a organização, não só em termos de longo prazo, mas porque uma ameaça, devido à falta de resiliência na organização, pode contribuir para uma quebra na entrega de serviço por um período prolongado. Da mesma forma que se considera que o planeamento é um elemento estratégico que permite o desenvolvimento de vantagens competitivas, também a *BCM* permite à organização preservar o valor oriundo de uma vantagem competitiva que também é estratégica (Herbane, Elliott, and Swartz 2004). Esta orientação estratégica é definida por Herbane, Elliot et al. (2004) como uma abordagem *business-driven*, baseada na combinação de planeamento e gestão que conduz, a longo prazo, à criação de valor e de vantagens para a organização.

A estratégia da organização em busca do objectivo referido decorre da abordagem efectuada e que depende do âmbito da actividade e da orientação da actividade (Figura 11)



Adaptado de (Herbane, Elliott, and Swartz 2004)

Figura 11 - Abordagens da continuidade.

A resposta a uma situação de crise depende do âmbito e da orientação da actividade, sendo que em qualquer dos casos ambas podem ser precursoras ou orientar-se para uma perspectiva estratégica. Sempre que uma organização segue um caminho com vista definição de um plano das interrupções técnicas (Plano de Recuperação de Desastres) ou um plano das interrupções sócio - técnicas (Plano de Continuidade do Negócio) em toda a organização, está a dar passos com vista à Gestão da Continuidade do Negócio.

### **2.3.2.1 Plano de Emergência**

Uma emergência é um evento não previsto que pode causar mortes ou lesões graves nos colaboradores, clientes ou público; pode causar o encerramento da organização ou a disrupção dos seus processos de negócio, provocar danos físicos ou ambientais ou prejudicar a situação financeira da organização e da sua imagem. As situações de crise podem ser variadas e ser desencadeadas por uma multiplicidade de factores, como por exemplo:

- Violência no espaço da organização;
- Acção terrorista;
- Extorsão;
- Falta de comunicação entre tecnologias;
- Substituição do Presidente do Conselho de Administração;
- Falhas de conformidade com regulamentação;
- Violação de informação privada;
- Sequestro;

As situações de crise podem surgir subitamente. Heath (2007) indica quatro factores que indicam a presença de uma situação de crise:

1. Informação desconhecida, duvidosa ou em falta;
2. Pouco tempo para decidir ou responder;
3. Uma ameaça para as pessoas ou recurso valioso para as pessoas;
4. Os recursos necessários para resolver a situação são superiores aos recursos existentes.

Uma crise pode causar outras situações de crise ou fazer emergir problemas críticos. Este “efeito cascata” (Heath 2007) pode ser resultado de uma má gestão da situação original de crise e estender os seus efeitos à organização e às pessoas e com impacto muito superior à situação que a despoletou.

O objectivo de um Plano de Emergência é o de minimizar as consequências negativas (por exemplo, perdas humanas e económicas) e de assegurar que a emergência não se vai transformar em desastre. Os eventos e as possibilidades de desastre que o Plano de Emergência pode accionar são difíceis de antecipar e podem ter consequências elevadas nos indivíduos e nos sistemas sociais. A falta de congruência entre os recursos disponíveis e as exigências colocadas para responder às necessidades podem ter consequências negativas em termos de stress ou mesmo gerar um sentimento de crise (Mendonca et al. 2006).

A resposta dos planos de emergência envolve a reacção a situações críticas. A gestão da crise assume dois tipos de desenvolvimentos: (Heath 2007) Gestão da Reacção – na resposta ao evento que despoletou a crise – e Gestão do Impacto – na forma como lida com o impacto nas pessoas e recursos que o evento despoletou. Estas duas abordagens colocam o seu foco nas

acções nos planos de pré-crise e de recuperação pós-crise, com menor ênfase na perspectiva da redução das situações que podem expor a organização à situação de crise.

A activação de um plano de emergência é baseada na avaliação dos impactos potenciais de um acidente e na avaliação das acções necessárias para eliminar ou, pelo menos, atenuar esses impactos. Quando os planos existentes são os adequados para uma situação de emergência, os resultados da aplicação verificam-se no tempo de reacção, na coordenação, em menos acidentes e na redução das perdas económicas. São necessárias abordagens flexíveis para a gestão da emergência de forma a garantir a segurança e uma resposta eficaz. Essa abordagem deve ser capaz de lidar com um ambiente de incerteza e mudança, permitir a revisão dos desenvolvimentos previstos na reacção e ser capaz de apoiar os gestores de emergência a improvisarem quando nenhum procedimento operacional padrão pode aliviar a catástrofe (Mendonça et al. 2006).

A elaboração de um plano de emergência pressupõe a identificação dos tipos de emergência potenciais e a definição das respostas a dar. A definição de emergência abre a porta a diversos tipos de eventos que podem gerar um impacto negativo nas pessoas e no negócio. A questão que se coloca é “Como podemos identificar os tipos de emergências mais susceptíveis de acontecer e que impacto terão na organização?” Na resposta a esta questão dúplice, Beatty propõe a construção de uma matriz de análise de vulnerabilidades (Tabela 1) que permite identificar, estimar a probabilidade, antecipar os impactos potenciais e o reconhecimento dos recursos, internos e externos, necessários para responder à emergência (2007).

Tabela 1 - Matriz de Análise de Vulnerabilidade

| Tipo de Emergência | Probabilidade |            | Impacto Humano       | Impacto Patrimonial | Impacto Negócio    | Recursos Internos   | Recursos Externos     | Total |
|--------------------|---------------|------------|----------------------|---------------------|--------------------|---------------------|-----------------------|-------|
|                    | Alta<br>5     | Baixa<br>1 | Elevado Impacto<br>5 |                     | Baixo Impacto<br>1 | Recursos Débeis (5) | Recursos Robustos (1) |       |
|                    |               |            |                      |                     |                    |                     |                       |       |

Adaptado de (Beatty 2007)

A existência de planos de emergência, com a descrição dos procedimentos, é importante para as organizações e os seus actores, constituindo modelos normativos para a educação e formação. Em particular servem de modelo para exercícios de simulação que, concomitantemente, são um meio de avaliação e melhoria dos planos de emergência.

### 2.3.2.2 Plano de Recuperação de Desastres

A literatura associa, com frequência, os conceitos de Recuperação de Desastres (*Disaster Recovery*) e de Continuidade do Negócio (Khorasani 2008), tratando-os como um componente do programa global de gestão dos recursos de informação (Raja and Kakoli 2000). Esta parece-nos uma associação demasiado redutora e conceptualmente limitadora da perspectiva holística que caracteriza a BCM.

Para o *Gartner Group* o BCP incorpora as orientações estratégicas no quadro de uma cultura corporativa, que abrangem uma série de táticas que ajudam a organização a mitigar os riscos que podem causar:

- Falhas nos processos de negócio;
- Perda de activos;
- Responsabilidade contratual;

- Falhas no serviço ao cliente;
- Danos na reputação e na marca;

enquanto que o *DRP* tem por missão a recuperação da tecnologia e das aplicações críticas da organização num *site* alternativo (Noakes-Fry and Diamond 2001). O *DRP* é desenvolvido na perspectiva dos cenários “*worst-case*”, ao invés do *BCP* que segue uma abordagem baseada em eventos específicos dentro da organização (Herbane, Elliott, and Swartz 2004).

Stanton (2005) segue esta dissociação, definindo o *DRP* como o processo habitualmente aplicado às TIC, que se desenrola durante e após uma crise na organização, ao invés do *BCP* que considera ser o processo que garante que a organização sobrevive a um evento que cause a disrupção e mitiga o seu impacto. O *BCP* é uma actividade que tem lugar antes de um incidente ocorrer e o *DRP* depois da sua ocorrência.

Uma ameaça pode materializar-se através de um ataque activo que contorne ou anule as medidas de protecção existentes. O objectivo da organização é o de identificar quando o processo de negócio tenha sido comprometido, tão cedo quanto possível, de forma a conter a ameaça reduzindo as possibilidades de ondulação e os efeitos de escalonamento (Gibb and Buchanan 2006). Nesta circunstância torna-se necessário iniciar um processo de recuperação do desastre e restabelecer o desempenho do processo ou do serviço. Um *DRP* deve especificar as políticas e procedimentos que devem ser desencadeados quando o desastre acontece. Gibb and Buchanan assinalam um conjunto de características a que deve obedecer um *DRP*:

- Definição de um canal de comunicação alternativo, pois na sequência de um desastre os canais convencionais de comunicação e de autorização podem não estar disponíveis;
- Alocação de um número de recursos mínimo (pessoal, instalações, *utilities*) necessário para o nível de serviço num tempo aceitável – *Recovery Time Objective (RTO)*;
- Ser parte do Manual de Continuidade da organização, incluindo os procedimentos para invocação do plano, um *site* seguro, preservação dos activos, etc.
- Fornecer a informação essencial, como, por exemplo, plantas e inventários de activos de informação, listas de pessoal, listas de sucessão, a equipas de recuperação, etc (2006).

O *DRP* deve estar ligado com a gestão global da continuidade do negócio, ser claro e conciso, focado nas actividades críticas da organização, ser testado e revisto com regularidade, ter um responsável reconhecido e cumprir os objectivos de recuperação. Os objectivos de recuperação comumente consagrados pelas boas práticas são:

- Objectivo do Tempo de Recuperação – *Recovery Time Objective (RTO)* – Quanto tempo pode o negócio funcionar sem os serviços críticos?
- Objectivo do Ponto de Recuperação – *Recovery Point Objective (RPO)* – A partir de que momento o ciclo de processamento vai ser recuperado? (Qual a quantidade de dados que pode perder-se ou ter de reintroduzir a partir de uma fonte alternativa?) Esta resposta pode ter várias opções:
  - o Zero perda de dados: recuperação até ao ponto de falha;
  - o Início do dia útil corrente – (*SoD – Start of Day*)
  - o Fim do dia útil anterior – (*EoD – End of Day*)
  - o O ponto entre o último *backup* disponível e o *SoD* ou *EoD* ou momento da falha;

Outro objectivo de medida a ter em conta é o Tempo Máximo de Interrupção Tolerável – *Maximum Tolerable Outage* – que é o tempo máximo que o negócio pode sobreviver desde a interrupção inicial. Estes objectivos devem ser objecto de análise rigorosa em sede de desenvolvimento da Análise de Impacto no Negócio (BIA).

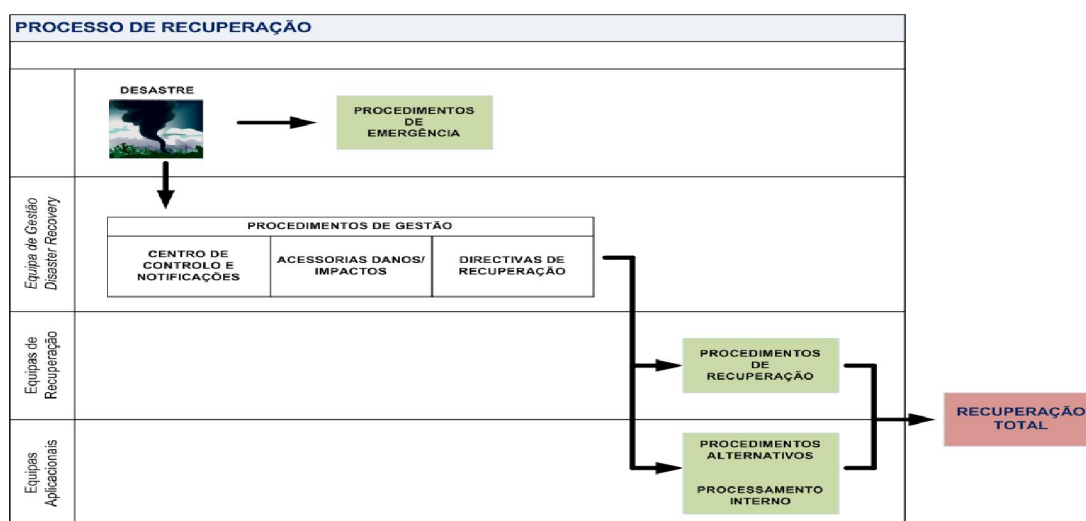


Figura 12 - Processo de Recuperação.

Sendo um processo reactivo, o *DRP* deve obedecer a uma sequencialidade de acções que visem o objectivo da recuperação total, com a seguinte sequência:

1. Ocorrência do desastre;
2. Evocação imediata dos procedimentos de emergência para a protecção de vidas e ao mesmo tempo minimizar o impacto do desastre;
3. A equipa de recuperação de desastres/continuidade do negócio é notificada e reúne num local predefinido para o efeito;
4. A equipa de recuperação de desastres/continuidade do negócio averigua os danos causados e avalia o impacto. Considera várias alternativas de recuperação e emite uma directiva de recuperação;
5. As equipas de recuperação entram em acção para restabelecer os procedimentos alternativos das aplicações críticas utilizando processos e recursos predefinidos e, se necessário, novas instalações;
6. As equipas aplicacionais iniciam o processamento alternativo das aplicações consideradas críticas, com a utilização dos procedimentos de recurso alternativos até a capacidade de processamento total ou parcial estar novamente disponível;
7. Assim que o processamento interino é estabelecido, a equipa de recuperação de desastres inicia os passos necessários para a restauração total e perfeita normalização das operações (Serrano and Jardim 2007).

### 2.3.2.3 Plano de Continuidade do Negócio

O risco é algo presente nas diversas componentes socioeconómicas do nosso quotidiano. A ausência de um *BCP* coloca as organizações na premência dos seguintes riscos (O'Hehir 2007):

- Interrupção da actividade resultando na incapacidade de satisfazer os seus clientes, na erosão da sua base de clientes, perda de oportunidades de negócio, perda de clientes e a incapacidade em competir com as outras organizações;
- Perdas financeiras devido à incapacidade de cobrar as facturas, atraso nos pagamentos e consequentes encargos em penalizações ou perda de descontos, incapacidade de manter os registos contabilísticos actualizados e perda de registos de vendas;
- Incapacidade de cumprir as obrigações legais ou de outras obrigações contratuais;
- Saída da actividade;

O *BCP* é muito mais um plano de gestão do que um plano técnico. Baseia-se na compreensão da organização, dos instrumentos que suportam as operações de negócio, da avaliação das possíveis falhas e do seu impacto (O'Hehir 2007) e tem por objecto a preservação dos activos de uma organização no caso da ocorrência de um desastre. Nesse desiderato convergem a capacidade da organização alcançar a sua missão, recuperar a sua operacionalidade, preservar a sua reputação e imagem, os seus clientes e a sua quota de mercado, em síntese, o seu lucro (Hiles 2007). No contexto actual em que vivemos, é fundamental as organizações ponderarem sobre a resposta a dar em caso da ocorrência de um desastre, com impacto em toda a actividade da organização ou na parcialidade dos seus processos de negócio.

Um *BCP* envolve organização, planeamento, formação, ensaio, ou seja, integrado plenamente num sistema de Gestão de Continuidade do Negócio (Cornish 2007). Na estruturação de um *BCP* existem diversas propostas de institutos de conformidade – *British Standards Institute*, *Disaster Recovery Institute International*, *itSMF International*, *Business Continuity Institute*, *CoBIT-Control Objectives for Information and related Technology*, *ISO – International Organization for Standardization* – que através dos standards e guias orientam as organizações no processo de desenvolvimento de um *BCP*.

A elaboração do *BCP*, como qualquer processo integrado e transversal, envolve um conjunto de passos, comumente aceites como boas práticas para o seu desenvolvimento. Zambon, Bolzoni et al (2007) seguem uma parte da metodologia proposta pelo standard BS25999 do *British Standards Institute (BSI)* e dividem a elaboração em 3 fases:

1. Identificação das actividades/processos que suportam os serviços críticos utilizados pela organização;
2. Identificação das relações/dependências entre as actividades/processos identificados;
3. Avaliação do impacto da disrupção dos serviços/processos críticos previamente identificados, mediante a *BIA*.

Pitt and Goyal (2004), Snedaker (2007) acompanham a metodologia do *Disaster Recovery Institute International (DRII)* dos Estados Unidos da América para a elaboração de um *BCP*:

1. Iniciação do Projecto, com o envolvimento de um Gestor Sénior e de um Comité de colaboradores dos diversos processos de negócio da organização;
2. Análise de Risco e do *BIA*, com o objectivo de determinar:

- 
- a. Requisitos e recursos críticos e os efeitos que um desastre possa ter nas pessoas, área de trabalho e processos,
  - b. Definir o tempo de recuperação para cada processo de negócio,
  - c. Estabelecer prioridades na recuperação,
  - d. Identificar o pessoal - chave, equipamentos e instalações,
  - e. Estimar os custos de interrupção dos processos de negócio e
  - f. Identificar os recursos necessários para desenvolver, testar e implementar o *BCP*;
3. Design e desenvolvimento do *BCP*, incluindo:
    - a. A estratégia, âmbito e objectivos do plano;
    - b. Procedimentos administrativos;
    - c. Formação do Comité de Continuidade e as equipas de suporte;
    - d. Linhas de comunicação, notificação e activação do plano;
    - e. Definição de cenários para o plano;
    - f. Registos, armazenamento, acesso ao *BCP* e
    - g. Orçamento do *BCP*.
  4. Criação do *BCP*, com a inclusão de:
    - a. Procedimentos de resposta de emergência que abrange a evacuação, decantação do acesso a áreas de trabalho, o acesso à documentação;
    - b. Centro de controlo de emergência - o estabelecimento, de comando e de controlo;
    - c. Procedimentos detalhados para as comunicações, a delegação / designação de autoridade, as principais partes interessadas;
    - d. Retoma detalhada, recuperação e procedimentos de restauração e
    - e. Recursos externos de apoio externo, os contratos de fornecedores, contactos.
  5. Testar e Exercitar o *BCP*, pois é essencial estabelecer a efectividade do *BCP* e implementar testes e exercícios regulares.
  6. Manutenção e Actualização do *BCP* com a incorporação dos resultados dos testes e exercícios, bem assim como auditorias independentes ao plano.

No capítulo 5 apresenta-se uma visão mais detalhada das várias propostas metodológicas dos standards de referência. As semelhanças entre o desenvolvimento de um *BCP* e a metodologia seguida no desenvolvimento de um projecto, reside no facto de qualquer plano dever seguir uma abordagem com início, meio e fim, e prever um programa de manutenção e de actualização em face das alterações tecnológicas e nos processos de negócio da organização.

## **2.4 Gestão da Continuidade do Negócio no contexto hospitalar**

A organização hospitalar, hospitais em particular, destaca-se das demais organizações pela criticidade da maioria dos serviços que presta e das dependências que estabelece com fornecedores de *utilities*. O tempo de *downtime* de um sistema, resultante de uma falha de energia, fornecimento de água, comunicações, etc., tem um impacto no serviço que, para além de económico, é fundamentalmente crítico face à indispensabilidade dos cuidados de saúde que presta.

Um dos sistemas mais críticos numa unidade de saúde é o fornecimento de energia eléctrica. Muitas instalações hospitalares não consideram incluir o

fornecimento de *backup* a todas as áreas, como por exemplo elevadores, sistemas HVAC, áreas conexas como o necrotério, etc. Da multiplicidade de sistemas que suportam a actividade hospitalar, destacam-se quatro que, em caso de falha podem comprometer a actividade de prestação de cuidados de saúde (Bierenbaum, Neiley, and Savageau 2009):

- Energia eléctrica de emergência;
- Sistemas de Comunicações;
- *Sites* alternativos;
- Armazenamento de Dados no exterior.

Embora a falha destes quatro sistemas críticos possa gerar o impasse nas actividades desenvolvidas dentro de um hospital, há muitos outros sistemas que precisam ser abordados, incluindo gases, vácuo, oxigénio, alarmes de incêndio, *sprinklers*, e a eliminação de resíduos.

A questão que se coloca é por que ordem de importância se deve considerar esta multiplicidade de factores e potenciais eventos? Bierenbaum, Neiley et al. (2009) sugerem um roteiro de nove etapas para atingir este desiderato:

1. Conhecer as capacidades e as limitações dos sistemas críticos da instituição.
2. Certificar-se que a avaliação de risco é conduzida para a mitigação dos efeitos das principais ameaças.
3. Desenvolver planos e projectos de mitigação e reforçar a resiliência.
4. Elaborar planos de emergência para o hospital e para cada departamento.
5. Comunicar a urgência destes sistemas para o fornecedor do serviço e verificar se é dada a prioridade na resposta e recuperação.
6. Formar todos os colaboradores de todos os departamentos. O Director clínico é um elemento chave no plano dos agentes da continuidade.
7. Realizar exercícios regulares envolvendo os sistemas críticos.
8. Utilizar os exercícios e experiências reais para aprender sobre todos os planos de continuidade dos sistemas críticos.
9. Rever o plano de continuidade anualmente, para garantir que está actualizado até à data.

Em Portugal, das vertentes abordadas, somente existe regulamentação sobre Segurança contra Incêndio em Edifícios, estabelecida pelo Decreto-Lei 220/2008, de 12 de Novembro, de forma a dotar estes edifícios de condições que reduzam os riscos de ocorrência de incêndio, garantam a segurança dos ocupantes e facilitem a intervenção dos bombeiros. A Portaria n.º 1532/2008, de 29 de Dezembro, institui o Regulamento técnico de segurança contra incêndio em edifícios, instituiu a obrigatoriedade da Organização de Segurança contra Incêndios, onde constam o Plano de Prevenção, **Plano de Emergência Interno**, Formação em Segurança contra Incêndio e os Simulacros. Estes normativos estabelecem:

- A acessibilidade e manobra dos meios de socorro ao edifício;
- A praticabilidade dos caminhos de evacuação;
- A eficácia dos meios de compartimentação, isolamento e protecção contra o fogo;
- A conservação e manutenção dos espaços e equipamentos;
- A limitação da utilização de substâncias perigosas e inflamáveis;
- As plantas e instruções de segurança;

- Instrução, formação e a realização de exercícios de segurança.

Em 2004, no quadro da preparação do Campeonato Europeu de Futebol - Euro 2004, as Administrações Regionais de Saúde determinaram a obrigatoriedade de todos os hospitais públicos estarem dotados de um Plano de Emergência Hospitalar, nas vertentes Interna e Externa, estando obrigados a obter a aprovação do plano, na vertente interna, pela Autoridade Nacional de Protecção Civil. O referencial para a elaboração do Plano de Emergência na vertente externa é uma publicação do Ministério da Saúde do Guia de Referência para a Elaboração de um Plano de Emergência Hospitalar.



### 3 Um retrato da continuidade do negócio nos hospitais em Portugal: Metodologia

Na decorrência da investigação sobre a temática da Gestão da Continuidade em contexto hospitalar, cedo deparamo-nos com a escassez de elementos quantitativos. O estudo mais recente sobre o estado dos sistemas de informação da saúde, conduzido por Luís Lapão em 2005 junto de hospitais públicos, revelou, entre outros, a baixa qualificação dos recursos humanos envolvidos neste sector e o baixo nível de maturidade dos sistemas de informação (Lapão 2007). Nesta área específica de investigação, não se encontrou qualquer estudo que retratasse a política da gestão da continuidade dos negócios nos hospitais em Portugal.

Neste contexto, a necessidade de promover um questionário nos hospitais portugueses, independentemente da personalidade jurídica ser pública, privada ou do terceiro sector, tornou-se premente. A motivação que presidiu a este questionário visou obter a resposta às seguintes questões de investigação:

1. Qual o grau de maturidade dos sistemas de informação dos hospitais em Portugal?
2. Qual a importância que as organizações hospitalares em Portugal dão à existência de uma política de gestão da continuidade do negócio?
3. Existe, está implementado ou qual o grau de implementação da gestão da continuidade do negócio e dos elementos que a compõe?
4. Que tipo de constrangimentos existem para a implementação de um plano de continuidade do negócio?

Neste capítulo apresenta-se a metodologia seguida na investigação, os critérios de selecção dos hospitais, os procedimentos adoptados para a recolha e processamento dos dados, bem assim como as limitações dos métodos utilizados e algumas considerações éticas.

#### 3.1 Abordagem Metodológica

A investigação visa a explicação, descrição ou previsão de contributos importantes e valiosos para a expansão do que sabemos e como vivemos nossas vidas. A investigação científica caracteriza-se pela abordagem metodológica e sistemática, e o método científico pela melhor abordagem para a aquisição de novos conhecimentos, porque fornece um conjunto de orientações sobre a recolha, avaliação e reporte da informação no contexto de uma pesquisa (Marczyk, DeMatteo, and Festinger 2005). A abordagem metodológica é, assim, uma das componentes de maior relevo num trabalho de investigação, pois é através dela que é descrito o percurso seguido na preparação do processo de investigação.

Sendo importante a metodologia na validação do estudo em questão, pretende-se contribuir para futuras investigações nesta área de conhecimento. Os aspectos metodológicos são, assim, uma etapa fundamental para o sucesso do trabalho.

Este estudo segue uma metodologia exploratória, descritiva e correlacional. É **exploratória**, no sentido *lato* - dado o ineditismo da investigação em Portugal - **descritiva** - porque procura especificar propriedades e características importantes do tema em estudo - e **correlacional**, porque procura avaliar a relação entre duas ou mais variáveis ou conceitos (Sampieri, Collado, and Lucio 2006).

O primeiro objectivo foi perceber o estado da arte da gestão de continuidade naquele contexto organizacional específico e no território português. Nesse desiderato promoveram-se entrevistas abertas com quadros hospitalares com responsabilidades na gestão dos sistemas de informação e gestão do risco. Na construção do guião da entrevista, servimo-nos de quatro questões de resposta aberta:

1. Qual o estado da arte dos sistemas de informação no hospital?
2. Está definida uma estratégia de continuidade no hospital? Em caso positivo, descreva-a. No caso negativo, há perspectivas para o seu desenvolvimento no futuro próximo?
3. Que instrumentos de resposta a uma situação de desastre tem o hospital e qual o grau de maturidade do processo no contexto organizacional?
4. Que mecanismos de segurança e protecção da informação estão implementados?

Da análise destas entrevistas e da revisão de literatura construiu-se o *corpus* do questionário (Anexo B) que foi enviado por via postal a 108 hospitais públicos, privados e do sector social.

Os questionários são confidenciais, não existindo qualquer menção à instituição questionada, tendo sido providenciado um envelope devidamente endereçado para remessa da resposta. Foi facultada a possibilidade das instituições hospitalares obterem uma cópia do relatório final resultante da análise do questionário e que será enviado após a apresentação pública deste estudo.

### 3.2 Universo e amostra

A população-alvo da pesquisa engloba todas as entidades prestadoras de cuidados de saúde e definidas como hospital – instituição de cuidados de saúde que presta tratamento médico e cirúrgico ao paciente, implicando, por vezes, o seu internamento.

A população-alvo das entidades públicas foi extraída a partir do Portal da Saúde (Saúde 2010) tendo sido aplicada a seguinte metodologia na construção da população-alvo:

- Centros Hospitalares – todos os Centros Hospitalares;
- Hospitais distritais – foram retirados os que integram Centros Hospitalares ou Unidades Locais de Saúde;
- Unidades Locais de Saúde – todas as Unidades Locais de Saúde;
- Maternidades - foram retiradas as que integram Centros Hospitalares;

Posteriormente foi segmentada de acordo com o regime jurídico da instituição como “Hospitais EPE”, para os hospitais com o estatuto de Entidade Pública Empresarial e “Outro”, para os demais hospitais públicos.

Relativamente aos Hospitais Privados e do Sistema Social, a população-alvo foi constituída a partir das organizações registadas na Entidade Reguladora da Saúde e que constam no respectivo *site* (<http://www.ers.min-saude.pt/>) aplicando o critério de selecção das entidades referenciadas como “Hospital”, “Misericórdia” e “Ordem”. A informação recolhida foi validada juntos dos *sites* de cada grupo empresarial, Santa Casa da Misericórdia ou Ordem Religiosa a quem pertencem os hospitais.

Aplicados os critérios expostos, a população-alvo ficou constituída pelos seguintes hospitais, distribuídos pela sua natureza jurídica:

Tabela 2 - Hospitais seleccionados por sector

|                           | N.º | %   |
|---------------------------|-----|-----|
| Hospitais EPE             | 49  | 45% |
| Outros Hospitais Públicos | 15  | 14% |
| Hospitais Privados        | 30  | 28% |
| Hospitais Sistema Social  | 14  | 13% |
| Total                     | 108 |     |

Os questionários foram dirigidos ao Presidente do Conselho de Administração, com uma carta de apresentação do questionário e dos seus objectivos (Anexo A), de 108 hospitais de Portugal e Regiões Autónomas dos Açores e da Madeira.

### 3.3 Recolha de dados

A recolha dos dados decorreu entre 15 Abril e 21 Junho de 2010. Durante este período foram contactados telefonicamente todos os hospitais para confirmação da recepção do questionário, tendo sido enviado, por correio electrónico, uma cópia do questionário sempre que não foi possível obter a confirmação.

Por duas vezes foi enviada uma mensagem via correio electrónico, solicitando a resposta ao questionário, sendo que na última comunicação foi adicionada uma hiperligação para resposta ao questionário por via electrónica (Alves 2010).

O canal preferencial para devolução do questionário foi a via postal, tendo três hospitais utilizado o correio electrónico e dois o preenchimento *on-line* no *site* indicado. Manifestaram interesse em obter o relatório da análise dos questionários sete hospitais.

### 3.4 Processamento dos dados

Os dados foram recolhidos para uma base de dados em MS Excel 2007, para uma análise de estatística descritiva e indutiva, aplicando para o efeito a técnica das tabelas dinâmicas disponível naquela tecnologia. Sempre que se entendeu necessário para sobrelevar alguma característica dos resultados, foram construídos tabelas e gráficos que serão incluídos na análise apresentada no próximo capítulo.

### 3.5 Limitações do método

A amostra é constituída por 46 respostas, representando 43% da população-alvo. A amostra de respostas obtidas é divergente na proporcionalidade de cada sector hospitalar na população-alvo.

Atendendo que o modelo de negócio, os objectivos, critérios de rentabilidade e modelos de gestão e os requisitos e obrigações legais são distintos, ou nem sempre consonantes, nos quatro tipos de hospital definidos, há algum risco que a inferência interpretativa sofra desvios resultantes destas diferentes características. Por exemplo, um hospital EPE, pela sua natureza de serviço público, está obrigado a disponibilizar um conjunto de serviços 24 x 7 que lhe exigem cuidados acrescidos na protecção e continuidade dos serviços, que um hospital social

ou privado não tem. No entanto, nas grandes linhas orientadoras que compõem uma política de gestão da continuidade do negócio, as exigências são semelhantes. Assim, sempre que a interpretação dos resultados globais não reflecte ou sofre desvios de incidência atendendo à tipologia de hospital, apresenta-se uma análise segmentada por natureza de hospital. Esta metodologia permite, por outro lado, uma análise comparativa *inter* e *intra* sectores hospitalares.

### **3.6 Considerações Éticas**

Os questionários são anónimos e confidenciais, e foi providenciado um envelope endereçado e sem remetente para a sua devolução. Devido à natureza sensível das informações colectadas durante este estudo e o potencial impacto sobre a organização, não haverá qualquer menção à origem da informação, mesmo nos casos em que seria possível registá-la.

Os resultados deste estudo serão tornados públicos através das entidades que revelem interesse em disponibilizar esta informação e junto de todos os hospitais que o solicitaram.

#### 4 Um retrato da continuidade do negócio nos hospitais em Portugal: Análise

Neste capítulo apresenta-se os resultados do questionário, de acordo com cada questão ou grupo homogéneo de questões e, sempre que se justifique, efectua-se uma correlação dos resultados obtidos.

A população - alvo é constituída por 108 hospitais a quem foram enviados os questionários e que foi seleccionada de acordo com a metodologia apresentada no capítulo anterior. A amostra obtida representa 43% dos hospitais consultados, segmentada de acordo com as seguintes classes, identificadas na questão.

Tabela 3 - Questionários enviados e recebidos

|                           | Enviados |     | Recebidos |     | Recebidos/Enviados |
|---------------------------|----------|-----|-----------|-----|--------------------|
|                           | N.º      | %   | N.º       | %   |                    |
| Hospitais EPE             | 49       | 45% | 18        | 40% | 37%                |
| Outros Hospitais Públicos | 15       | 14% | 6         | 13% | 40%                |
| Hospitais Privados        | 30       | 28% | 16        | 36% | 53%                |
| Hospitais Sistema Social  | 14       | 13% | 5         | 11% | 36%                |
| Não Identificado          |          |     | 1         |     |                    |
| Total                     | 108      |     | 46        | 43% |                    |

A representação dos hospitais na população – alvo é de 45%, 28%, 14% e 13% para os hospitais EPE, hospitais privados, outros hospitais do SNS, e hospitais do sistema social respectivamente. Na amostra em análise a representação alterou-se substancialmente, passando a ser de 53%, 40%, 37% e 36% para os hospitais privados, outros hospitais públicos, hospitais EPE e hospitais do sistema social respectivamente. Comparando a segmentação dos hospitais na população – alvo com a da amostra, verifica-se que o contributo dos hospitais privados na amostra foi superior à sua representação na população – alvo. Nos outros hospitais públicos e do sector social a proporção mantém-se e nos hospitais EPE fica aquém da sua representação na população-alvo.

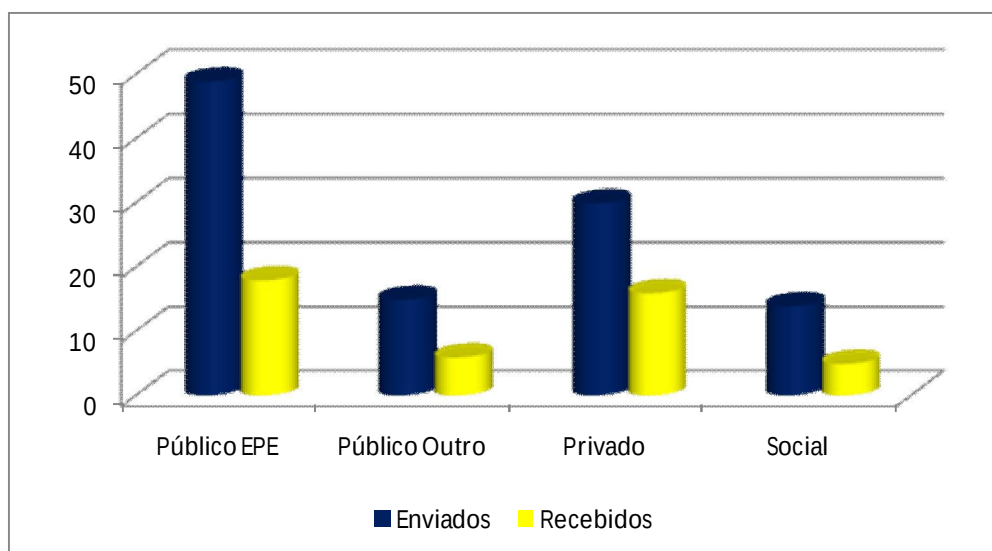


Figura 13 - Relação de questionários enviados e recebidos

#### 4.1 Dimensão através do n.º de camas de internamento

Utilizando o n.º oficial de camas para internamento como indicador da dimensão do hospital, distribuídas por 5 classes, observaram-se os seguintes resultados:

Tabela 4 - N.º oficial de camas por natureza de hospital

|                          | ?        |           | <100      |            | 100-250   |            | 250-500  |            | 500-1000 |           | >1000    |           |
|--------------------------|----------|-----------|-----------|------------|-----------|------------|----------|------------|----------|-----------|----------|-----------|
|                          | Nº       | %         | Nº        | %          | Nº        | %          | Nº       | %          | Nº       | %         | N        | %         |
| Hospitais EPE            | 0        | 0%        | 0         | 0%         | 6         | 40%        | 6        | 67%        | 4        | 100%      | 2        | 100%      |
| Outros Hospitais         | 0        | 0%        | 3         | 23%        | 2         | 13%        | 1        | 11%        | 0        | 0%        | 0        | 0%        |
| Hospitais Privados       | 2        | 13%       | 8         | 62%        | 5         | 33%        | 1        | 11%        | 0        | 0%        | 0        | 0%        |
| Hospitais Sistema Social |          | 0%        | 2         | 15%        | 2         | 13%        | 1        | 11%        | 0        | 0%        | 0        | 0%        |
| Não Identificado         | 1        | -         | -         | -          | -         | -          | -        | -          | -        | -         | -        | -         |
| <b>Total</b>             | <b>3</b> | <b>7%</b> | <b>13</b> | <b>30%</b> | <b>15</b> | <b>35%</b> | <b>9</b> | <b>21%</b> | <b>4</b> | <b>9%</b> | <b>2</b> | <b>5%</b> |

Relativamente à dimensão dos hospitais, 86% tem menos de 500 camas de internamento e somente os hospitais EPE dispõe de capacidade igual ou superior às 500 camas. Dos hospitais EPE, 33% dispõe de mais do que 500 camas, todos com mais do que 100 camas, o que se justifica pelo facto de 47% estarem agrupados em Centros Hospitalares que agregam vários hospitais e é utilizado o número total de camas como indicador de referência do Centro Hospitalar.

Na perspectiva da natureza do hospital, 81% dos hospitais privados têm um n.º de camas inferior a 250, sendo que 50% não dispõe de mais do que 100 camas. Os hospitais do Sistema Social, acompanham os hospitais privados (e vice-versa) na sua dimensão até às 250 camas, destacando-se a representação para a classe das [250-500].

Tabela 5 - Representação da dimensão por tipo de hospital

|               | <100 | 100-250 | 250-500 | 500-1000 | >1000 |
|---------------|------|---------|---------|----------|-------|
| Privado       | 50%  | 31%     | 6%      | 0%       | 0%    |
| Social        | 40%  | 40%     | 20%     | 0%       | 0%    |
| Público EPE   | 0%   | 33%     | 33%     | 22%      | 11%   |
| Público Outro | 50%  | 33%     | 17%     | 0%       | 0%    |

Em conclusão, relativamente à proposta de serviço dos hospitais aferida pela disponibilidade de internamento, os hospitais sociais e privados disponibilizam um reduzido n.º de camas, sendo que contribuem para 77% dos hospitais com menos do que 100 camas. Os hospitais EPE, em regra hospitais centrais ou distritais têm uma maior disponibilidade de camas, sendo que os hospitais públicos com menos de 100 camas, são hospitais que ainda não foram integrados em Centros Hospitalares ou Unidades Locais de Saúde.

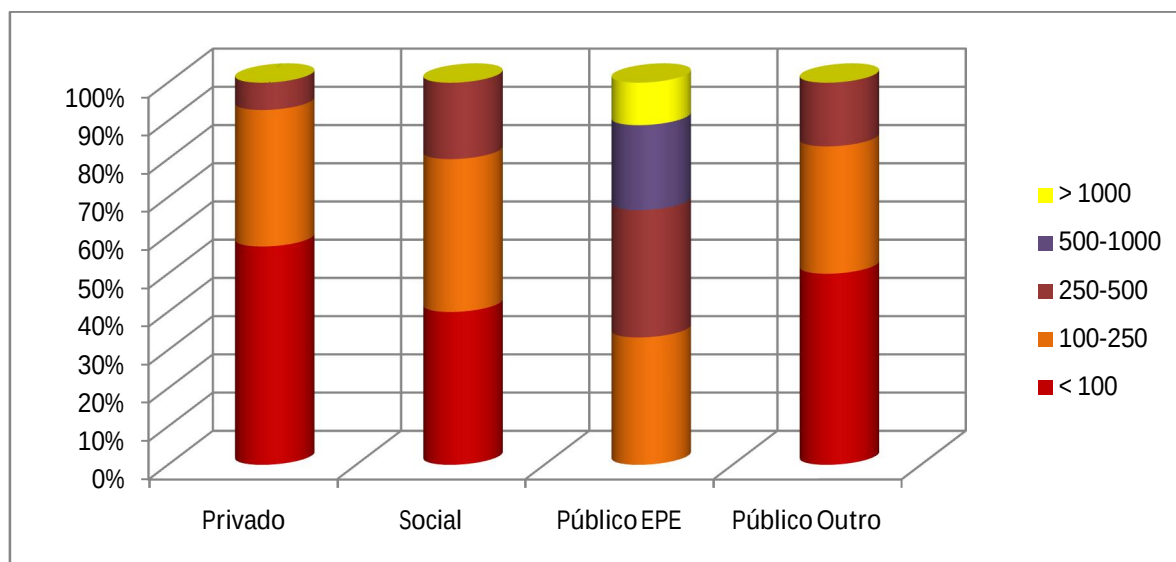


Figura 14 - N.º de Camas por Natureza de hospital

#### 4.2 Valências de Serviço

Reflectindo sobre a oferta de cuidados de saúde, os hospitais foram questionados sobre as valências de serviço existente no hospital. Da recolha das principais actividades hospitalares ou das mais genéricas, resultou a seguinte lista:

- ☐ Cirurgia
- ☐ Medicina
- ☐ Mulher e Criança
- ☐ Urgência
- ☐ Saúde Mental
- ☐ Consulta Externa
- ☐ Meios Complementares de Diagnóstico e Tratamento
- ☐ Ambulatório
- ☐ Hospital de Dia

possibilitando-se a inclusão de valências que não figurassem no questionário. Da recolha resultou a seguinte distribuição:

Tabela 6 - Distribuição de Valências de Serviço por natureza de hospital

|               | Cirurgia | Urgência | MCDT | Medicina | Saúde Mental | Ambulatório | Mulher e Criança | Consulta Externa | Hospital de Dia | UCCI | MFR | AMP | Ortopedia |
|---------------|----------|----------|------|----------|--------------|-------------|------------------|------------------|-----------------|------|-----|-----|-----------|
| Público EPE   | 18       | 17       | 18   | 18       | 15           | 17          | 15               | 18               | 18              | 2    | 1   | 0   | 2         |
| Público Outro | 4        | 1        | 5    | 3        | 1            | 5           | 1                | 5                | 2               | 2    | 1   | 0   | 1         |
| Privado       | 15       | 6        | 14   | 11       | 1            | 13          | 6                | 14               | 6               | 0    | 1   | 2   | 1         |
| Social        | 5        | 2        | 4    | 4        | 0            | 5           | 1                | 4                | 1               | 2    | 0   | 1   | 0         |
| Total         | 42       | 26       | 41   | 36       | 17           | 40          | 23               | 41               | 27              | 6    | 3   | 3   | 4         |

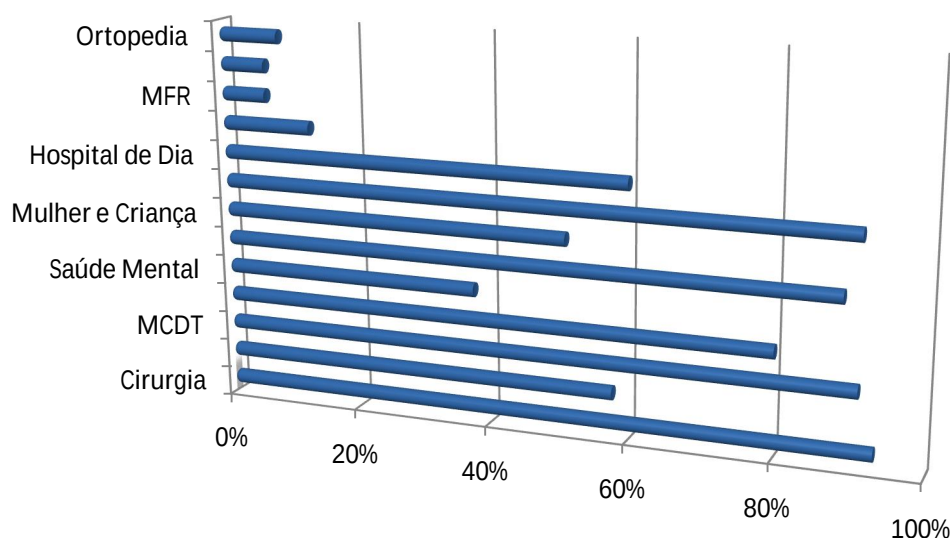


Figura 15 - Oferta de Cuidados de Saúde pelas diversas valências

As valências de Cirurgia, Meios Complementares de Diagnóstico e Tratamento, Ambulatório e Consulta Externa são disponibilizadas por mais de 90% dos hospitais, independentemente da natureza da propriedade.

Analisando por natureza de hospital, verifica-se que os Hospitais EPE têm uma oferta de serviço universal, cobrindo todas as valências indicadas, com ligeira quebra na valência “Saúde Mental” e “Mulher e Criança”. A quebra na valência “Saúde Mental” é mais acentuada nos restantes hospitais, pois estes cuidados de saúde são quase exclusivamente prestados pelos Hospitais EPE.

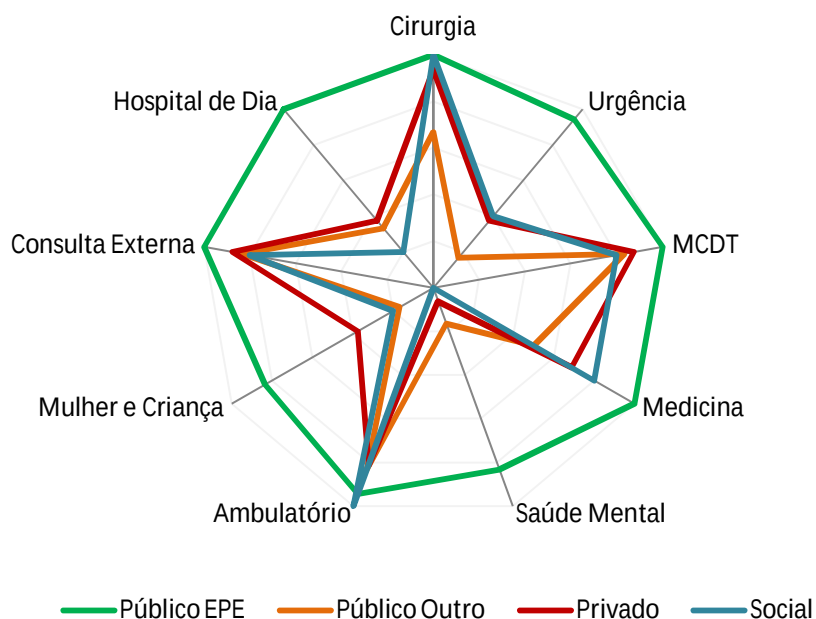


Figura 16 - Distribuição das valências por natureza de hospital

### 4.3 Maturidade dos sistemas de informação hospitalares

Para a obtenção deste indicador, foi utilizada como referência a Matriz de Maturidade dos Sistemas de Informação para Hospitais desenvolvida pela IDC (IDC 2008). Utilizou-se esta matriz como referência pelo facto de ser conhecida pelos hospitais e identificar claramente as diversas soluções disponíveis nas TI da saúde. Esta matriz define 5 estágios de maturidade dos SI já referidos no capítulo 2.1.1 - Os HIS, que comportam um conjunto de aplicações cujo utilização prefigura a pertença integral ou parcial a esse estágio de maturidade (Anexo B – Questão Q4)

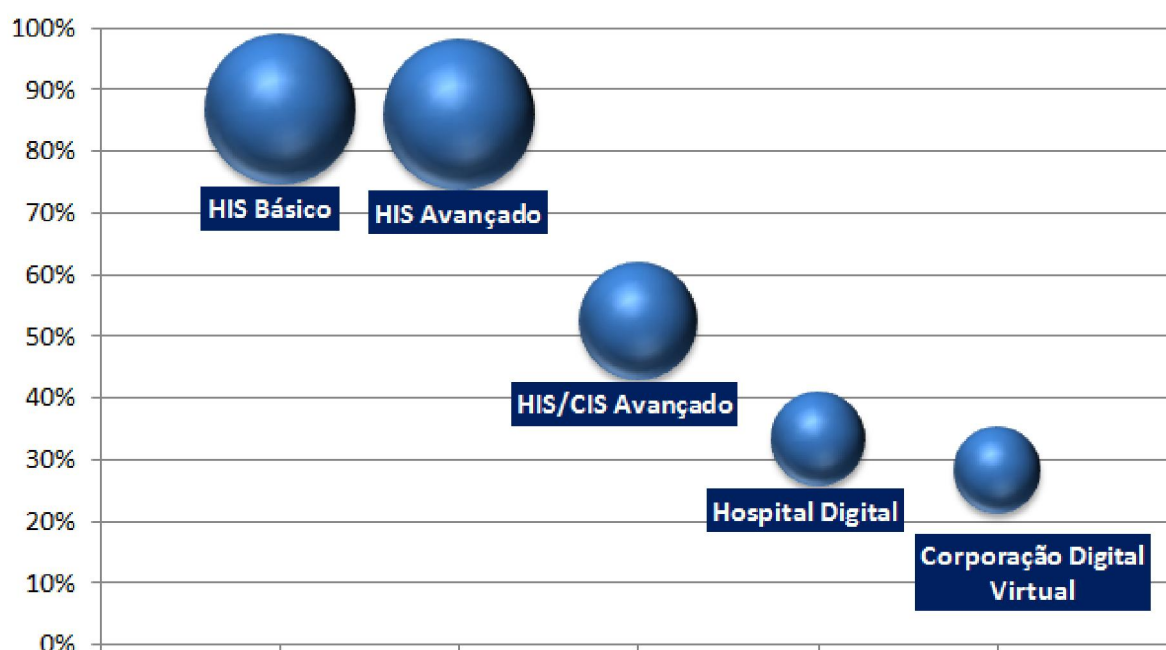


Figura 17 - Maturidade dos SI nos Hospitais Portugueses

A maturidade dos SI dos hospitais portugueses reflecte as características de um HIS Avançado, independentemente da natureza do hospital, sendo esta realidade mais efectiva nos hospitais do SNS. Relativamente aos estágios superiores da matriz, os hospitais EPE assumem notoriamente a liderança

Tabela 7 - Comparação da Maturidade dos SI no Hospitais

|                                   | Social | Privados | EPE        | Outro      |
|-----------------------------------|--------|----------|------------|------------|
| <b>HIS Básico</b>                 | 82%    | 82%      | <b>91%</b> | 90%        |
| <b>HIS Avançado</b>               | 72%    | 80%      | <b>92%</b> | <b>92%</b> |
| <b>HIS/CIS Avançado</b>           | 40%    | 36%      | <b>72%</b> | 43%        |
| <b>Hospital Digital</b>           | 9%     | 26%      | <b>44%</b> | 38%        |
| <b>Corporação Digital Virtual</b> | 13%    | 25%      | <b>38%</b> | 19%        |

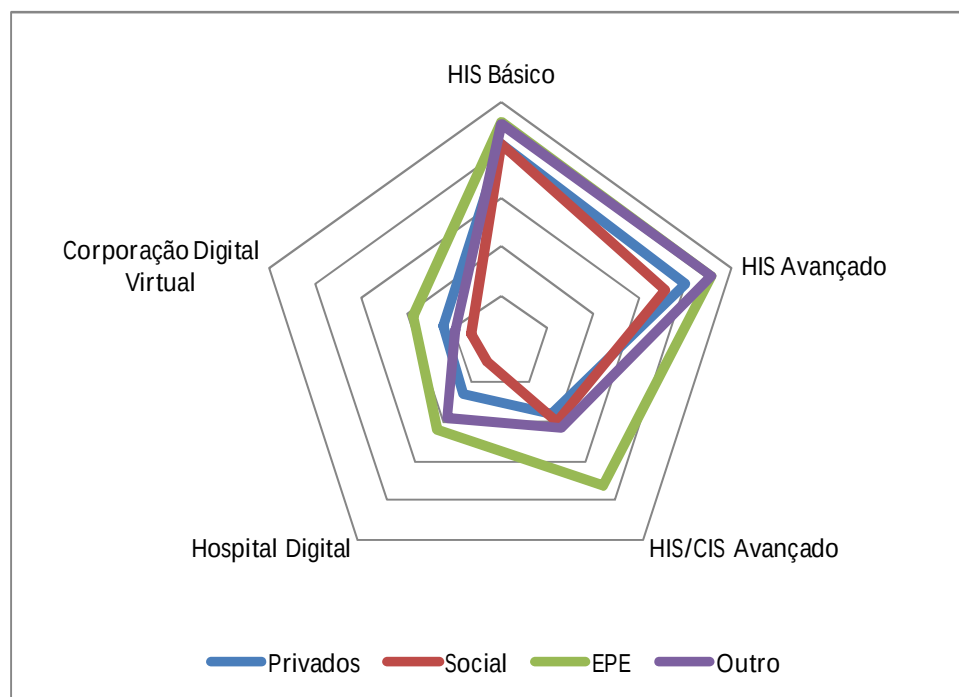


Figura 18 - Comparação da Maturidade dos SI no Hospitais

Analisando cada um dos componentes que define o estágio de maturidade, na tabela 8 apresenta-se o rácio de hospitais, de cada sector, que dispõe dessa tecnologia. Dos resultados destaca-se a liderança dos Hospitais EPE na desmaterialização dos processos e da integração das TI nas principais actividades ordinárias, quer de *back-office*, quer na prestação efectiva de cuidados de saúde.

Tabela 8 – Taxa de Implementação das Aplicações nos Hospitais

|                  |                                                       | Privado | Social | Público EPE | Público Outro |
|------------------|-------------------------------------------------------|---------|--------|-------------|---------------|
| HIS BÁSICO       | Registo de doentes                                    | 100%    | 100%   | 100%        | 86%           |
|                  | Facturação                                            | 88%     | 75%    | 94%         | 86%           |
|                  | Contas correntes                                      | 81%     | 75%    | 89%         | 71%           |
|                  | Contabilidade                                         | 88%     | 100%   | 100%        | 86%           |
|                  | Salários                                              | 88%     | 100%   | 94%         | 86%           |
|                  | Ferramentas de escritório electrónico                 | 69%     | 75%    | 83%         | 57%           |
|                  | LAN                                                   | 63%     | 50%    | 78%         | 71%           |
| HIS AVANÇADO     | Agendamento de actos médicos                          | 100%    | 100%   | 94%         | 86%           |
|                  | Registo de actos médicos                              | 88%     | 75%    | 94%         | 86%           |
|                  | Gestão do arquivo clínico                             | 44%     | 25%    | 72%         | 43%           |
|                  | Logística                                             | 69%     | 75%    | 94%         | 71%           |
|                  | Gestão de stocks                                      | 88%     | 75%    | 94%         | 86%           |
|                  | Correio electrónico                                   | 100%    | 100%   | 100%        | 86%           |
|                  | Acesso à internet                                     | 100%    | 100%   | 94%         | 86%           |
| HIS/CIS AVANÇADO | Intranet                                              | 56%     | 25%    | 89%         | 86%           |
|                  | LIS – <i>Laboratory Information System</i>            | 25%     | 50%    | 94%         | 29%           |
|                  | RIS – <i>Radiology Information System</i>             | 44%     | 25%    | 89%         | 57%           |
|                  | Bloco Operatório                                      | 63%     | 50%    | 78%         | 29%           |
|                  | Extranet – EDI                                        | 6%      | 25%    | 6%          | 14%           |
|                  | PACS – <i>Picture Archiving and Computing Systems</i> | 44%     | 50%    | 94%         | 57%           |

|                            |                                                  |     |     |     |     |
|----------------------------|--------------------------------------------------|-----|-----|-----|-----|
| HOSPITAL DIGITAL           | Processo Clínico Electrónico                     | 44% | 25% | 44% | 43% |
|                            | Prescrição electrónica                           | 31% | 0%  | 89% | 71% |
|                            | Notas de enfermagem                              | 56% | 0%  | 72% | 57% |
|                            | Portal do doente                                 | 6%  | 0%  | 17% | 0%  |
|                            | Portal colaborativo                              | 19% | 0%  | 28% | 14% |
|                            | WLAN                                             | 19% | 25% | 50% | 29% |
|                            | Ferramentas colaborativas                        | 19% | 0%  | 33% | 29% |
|                            | Wireless point of care                           | 13% | 25% | 22% | 14% |
| CORPORAÇÃO DIGITAL VIRTUAL | Sistemas de informação de Gestão (Datawarehouse) | 31% | 25% | 50% | 29% |
|                            | Portais de saúde                                 | 13% | 0%  | 22% | 43% |
|                            | Sistemas de apoio à decisão clínica              | 6%  | 0%  | 28% | 14% |
|                            | Videoconferência                                 | 38% | 0%  | 33% | 0%  |
|                            | Segurança                                        | 31% | 25% | 61% | 14% |
|                            | WAN                                              | 31% | 25% | 33% | 0%  |

Da análise pode-se inferir o *ranking* de cada uma das soluções aplicacionais na globalidade dos SI disponíveis e que, de alguma forma, indica a estratégia de integração dos SI nos hospitais:

Tabela 9 - *Ranking* das Soluções de TI

| Privado                                        | Social                                         | Público EPE                                    | Público Outro                                  |
|------------------------------------------------|------------------------------------------------|------------------------------------------------|------------------------------------------------|
| Registo de doentes                             | Registo de doentes                             | Registo de doentes                             | Registo de doentes                             |
| Agendamento de actos médicos                   | Contabilidade                                  | Contabilidade                                  | Facturação                                     |
| Correio electrónico                            | Salários                                       | Correio electrónico                            | Contabilidade                                  |
| Acesso à internet                              | Agendamento de actos médicos                   | Facturação                                     | Salários                                       |
| Facturação                                     | Correio electrónico                            | Salários                                       | Agendamento de actos médicos                   |
| Contabilidade                                  | Acesso à internet                              | Agendamento de actos médicos                   | Registo de actos médicos                       |
| Salários                                       | Facturação                                     | Registo de actos médicos                       | Gestão de stocks                               |
| Registo de actos médicos                       | Contas correntes                               | Logística                                      | Correio electrónico                            |
| Gestão de stocks                               | Ferramentas de escritório electrónico          | Gestão de stocks                               | Acesso à internet                              |
| Contas correntes                               | Registo de actos médicos                       | Acesso à internet                              | Intranet                                       |
| Ferramentas de escritório electrónico          | Logística                                      | LIS – Laboratory Information System            | Contas correntes                               |
| Logística                                      | Gestão de stocks                               | PACS – Picture Archiving and Computing Systems | LAN                                            |
| LAN                                            | LAN                                            | Contas correntes                               | Logística                                      |
| Bloco Operatório                               | LIS – Laboratory Information System            | Intranet                                       | Prescrição electrónica                         |
| Intranet                                       | Bloco Operatório                               | RIS – Radiology Information System             | Ferramentas de escritório electrónico          |
| Notas de enfermagem                            | PACS – Picture Archiving and Computing Systems | Prescrição electrónica                         | RIS – Radiology Information System             |
| Gestão do arquivo clínico                      | Gestão do arquivo clínico                      | Ferramentas de escritório electrónico          | PACS – Picture Archiving and Computing Systems |
| RIS – Radiology Information System             | Intranet                                       | LAN                                            | Notas de enfermagem                            |
| PACS – Picture Archiving and Computing Systems | Processo Clínico Electrónico                   | Bloco Operatório                               | Gestão do arquivo clínico                      |
| Processo Clínico Electrónico                   | WLAN                                           | Gestão do arquivo clínico                      | Processo Clínico Electrónico                   |
| Videoconferência                               | Sistemas de informação de Gestão               | Notas de enfermagem                            | Portais de saúde                               |
| Prescrição electrónica                         | RIS – Radiology Information System             | Segurança                                      | LIS – Laboratory Information System            |
| Sistemas de informação de Gestão               | Extranet – EDI                                 | WLAN                                           | Bloco Operatório                               |
| Segurança                                      | Prescrição electrónica                         | Sistemas de informação de Gestão               | WLAN                                           |
| WAN                                            | Notas de enfermagem                            | Processo Clínico Electrónico                   | Ferramentas colaborativas                      |
| LIS – Laboratory Information System            | Wireless point of care                         | Ferramentas colaborativas                      | Sistemas de informação de Gestão               |
| Portal colaborativo                            | Segurança                                      | Videoconferência                               | Extranet – EDI                                 |
| WLAN                                           | WAN                                            | WAN                                            | Portal colaborativo                            |
| Ferramentas colaborativas                      | Portal do doente                               | Portal colaborativo                            | Wireless point of care                         |
| Wireless point of care                         | Portal colaborativo                            | Sistemas de apoio à decisão clínica            | Sistemas de apoio à decisão clínica            |
| Portais de saúde                               | Ferramentas colaborativas                      | Wireless point of care                         | Segurança                                      |
| Extranet – EDI                                 | Portais de saúde                               | Portais de saúde                               | Portal do doente                               |
| Portal do doente                               | Sistemas de apoio à decisão clínica            | Portal do doente                               | Videoconferência                               |
| Sistemas de apoio à decisão clínica            | Videoconferência                               | Extranet – EDI                                 | WAN                                            |

Os hospitais públicos seguiram a implementação sequenciada pelos estágios de maturidade definidos pela matriz IDC. Os hospitais privados, de implementação mais recente, revelam maior prioridade às soluções incluídas no estágio “HIS Avançado”. O mesmo se verifica nos hospitais do sistema social, ainda que de forma atenuada e mesclada. A partir do último terço do *ranking* a estratégia de implementação é comum a todos os hospitais.

Caracterizada que está a amostra relativamente à tipologia, dimensão e nível de maturidade dos SI dos hospitais consultados, a análise que a seguir se apresenta reflecte as perspectivas dos diversos hospitais relativamente à temática objecto de estudo.

#### 4.4 Importância da Continuidade do Negócio no serviço hospitalar

Questionados sobre a importância atribuída à Gestão da Continuidade do Negócio, inquestionavelmente, 98% dos hospitais consideram a BCM como um assunto muito importante (76%) ou importante (22%).

Tabela 10 – Grau de Importância da Gestão da Continuidade do Negócio

|                  | N.º | %   |
|------------------|-----|-----|
| Muito Importante | 35  | 76% |
| Importante       | 10  | 22% |
| Pouco Importante | 0   | 0%  |
| Nada Importante  | 0   | 0%  |
| Não respondeu    | 1   | 2%  |

Relativamente à questão da condução da política de continuidade, 86% dos hospitais responderam “Conselho de Administração”, confirmando a teoria de que este é um processo holístico de gestão e, como tal, deve ser conduzido pela administração da organização, sem prejuízo do envolvimento de outras unidades orgânicas.

Tabela 11 - Condução da Política de BCM

|                                | N.º | %   |
|--------------------------------|-----|-----|
| Conselho de Administração      | 36  | 86% |
| Direcção de Risco              | 3   | 7%  |
| Equipa Técnica Específica      | 2   | 5%  |
| Direcção de SI                 | 1   | 2%  |
| Dir. de Equipam. e Instalações | 0   | 0%  |
| Gestor Sénior                  | 0   | 0%  |
| Outro                          | 0   | 0%  |
| Não respondeu                  | 3   | 7%  |

#### 4.5 Percepção dos Riscos potenciais

No que concerne à percepção do risco, foi apresentada a seguinte lista de riscos potenciais, solicitando a atribuição de uma pontuação de acordo com a sua percepção do impacto desse risco na organização:

- Ameaças Electrónicas
- Ameaças Atmosféricas
- Inundações
- Falhas na Logística
- Acidentes
- Doenças
- Ameaças à Infra-estrutura
- Incêndios
- Greves de Pessoas
- Assaltos

da qual resultou a seguinte matriz de avaliação:

Tabela 12 - Percepção do Risco

|                           | Privado | Social | EPE | Outro |
|---------------------------|---------|--------|-----|-------|
| Ameaças Electrónicas      | 3º      | 6º     | 5º  | 1º    |
| Doenças                   | 4º      | 4º     | 2º  | 1º    |
| Ameaças Atmosféricas      | 9º      | 6º     | 7º  | 8º    |
| Ameaças à Infra-estrutura | 5º      | 5º     | 4º  | 4º    |
| Inundações                | 7º      | 6º     | 7º  | 8º    |
| Incêndios                 | 1º      | 1º     | 1º  | 4º    |
| Falhas na Logística       | 1º      | 1º     | 2º  | 3º    |
| Greves de Pessoas         | 8º      | 3º     | 6º  | 4º    |
| Acidentes                 | 6º      | 6º     | 9º  | 7º    |
| Assaltos                  | 10º     | 10º    | 10º | 10º   |

De salientar a importância atribuída aos “Incêndios”, “Falhas na Logística”, “Ameaças electrónicas (vírus)” e “Doenças (pandemias)” em todos os hospitais e a baixa importância atribuída ao risco de “Assalto”.

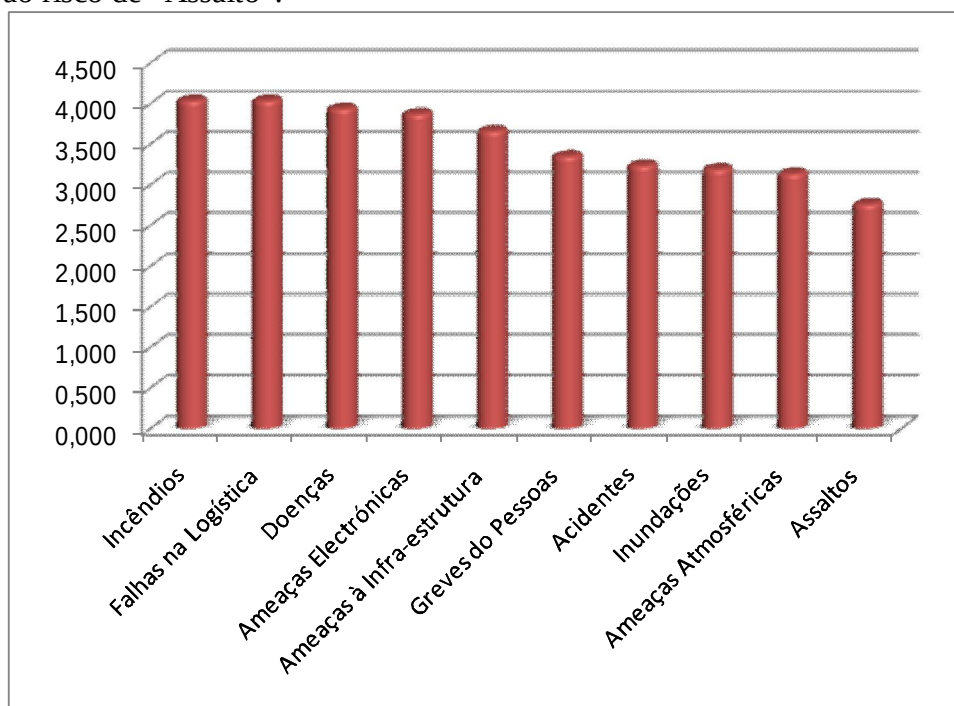


Figura 19 - Percepção do Risco no Negócio Hospitalar

#### 4.6 Quebras de Serviço e Impacto no Negócio

As questões seguintes visam obter informação sobre a ocorrência de quebras de serviço e do seu registo e contabilização do impacto no negócio. À pergunta se havia registo de quebras de serviço em n.º de dias, devidas a falhas não programadas, no ano de 2009, as respostas dividiram-se em igual proporção.

Analisando as respostas de cada hospital, ponderadas pelo n.º de respostas obtidas por hospitais da mesma natureza, os hospitais EPE e do sistema social declararam um maior n.º de registos de quebras de serviço motivadas por falhas não planeadas, numa relação quase proporcionalmente inversa à inexistência de registos por parte dos hospitais privados e outros hospitais públicos.

Tabela 13 - Registo de Quebras de Serviço

|               | Privado |     | Social |     | EPE |     | Outro |     |
|---------------|---------|-----|--------|-----|-----|-----|-------|-----|
| Não           | 11      | 69% | 1      | 20% | 5   | 28% | 5     | 83% |
| Sim           | 5       | 31% | 3      | 60% | 13  | 72% | 0     | 0%  |
| Não respondeu | 0       | 0%  | 0      | 0%  | 0   | 0%  | 1     | 17% |

Relativamente ao impacto das quebras em termos de interrupção do serviço, foram registadas as seguintes quebras de serviço em n.º de dias:

Tabela 14 - N.º de dias de quebras de serviço registados

|               | Privado | Social | EPE | Outro |
|---------------|---------|--------|-----|-------|
| < 1           | 2       | 3      | 8   | 2     |
| 1 – 2         | 1       |        | 4   | 1     |
| 3 – 5         | 1       |        | 1   | 1     |
| Indeterminado | 1       |        |     | 1     |

Em termos financeiros, somente um hospital EPE determinou o custo do impacto da quebra de serviço, que orçou cerca de vinte mil euros. As causas da quebra de serviço identificadas e o n.º de ocorrências foi de:

Tabela 15 - Causas das Quebras de Serviço e n.º de ocorrências

|                                   | Privado | Social | EPE |
|-----------------------------------|---------|--------|-----|
| Falhas dos Sistema de TI          | 30      | 19     | 22  |
| Condições Atmosféricas            | 12      | 0      | 4   |
| Falha de Pessoas                  | 21      | 1      | 8   |
| Falha nas Comunicações            | 26      | 5      | 9   |
| Falta de água, luz, gás, ...      | 21      | 1      | 11  |
| Doença de colaboradores           | 1       | 1      | 0   |
| Falta de competências chave       | 20      | 0      | 12  |
| Incêndio                          | 0       | 0      | 0   |
| Falha no abastecimento            | 0       | 0      | 1   |
| Paralisação do Equipamento Médico | 0       | 0      | 1   |

As falhas dos sistemas de TI, as falhas nas comunicações, a falta de água, luz, gás, ..., a falha de pessoas e a falta de competências chave registam o maior n.º de ocorrências.

Questionados sobre o tipo de riscos que estão cobertos pela política de Continuidade do Negócio do hospital, foram assinalados os seguintes:

Tabela 16 - Riscos cobertos pelos Planos de Continuidade de Negócio

|                              |     |                             |     |
|------------------------------|-----|-----------------------------|-----|
| Falhas dos Sistema de TI     | 1 º | Falha nas Comunicações      | 2 º |
| Falta de água, luz, gás, ... | 3 º | Falha de Pessoas            | 4 º |
| Incêndio                     | 5 º | Falha no abastecimento      | 5 º |
| Doença de colaboradores      | 7 º | Condições Atmosféricas      | 8 º |
|                              |     | Falta de competências chave | 8 º |

Os próximos três subcapítulos analisam a implementação dos três componentes da Gestão da Continuidade do Negócio, identificadas no capítulo 2:

- Plano de Continuidade do Negócio – *BCP – Business Continuity Planning*
- Plano de Recuperação de Desastres – *DR – Disaster Recovery*
- Plano de Emergência – *EP – Emergency Planning*

#### 4.7 Plano de Continuidade do Negócio e os seus componentes

O *BCP* é um dos instrumentos que consubstancia a aplicação de uma política integrada e holística da Gestão da Continuidade do Negócio, referida como muito importante ou importante por 98% dos hospitais consultados.

Neste subcapítulo apresenta-se a análise das respostas dos hospitais. Procurando validar a importância atribuída pelos hospitais à implementação de um *BCP*, verifica-se que 43% consideram-no “Muito Importante”, 39% “Importante”, 9% “Pouco importante” e 9% não manifestaram opinião.

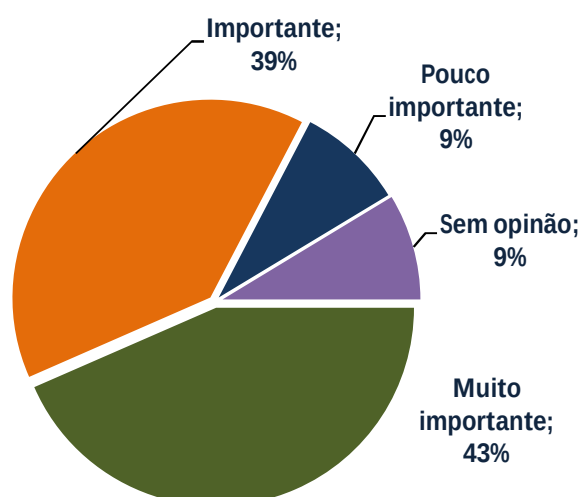


Figura 20 - Importância do Plano de Continuidade do Negócio

Segmentando estes resultados de acordo com a natureza dos hospitais, os resultados são os seguintes:

Tabela 17 - Importância da existência de um *BCP*

|               | Muito Importante | Importante | Pouco Importante | Sem Opinião |
|---------------|------------------|------------|------------------|-------------|
| Público EPE   | 56%              | 44%        |                  |             |
| Público Outro | 17%              | 33%        | 17%              | 33%         |
| Privado       | 38%              | 31%        | 18%              | 13%         |
| Social        | 60%              | 40%        |                  |             |

Questionados sobre a efectividade do desenvolvimento e implementação de um *BCP*, 83% responderam que não têm implementado um *BCP*. Os 17% que responderam afirmativamente estão distribuídos pelos seguintes hospitais:

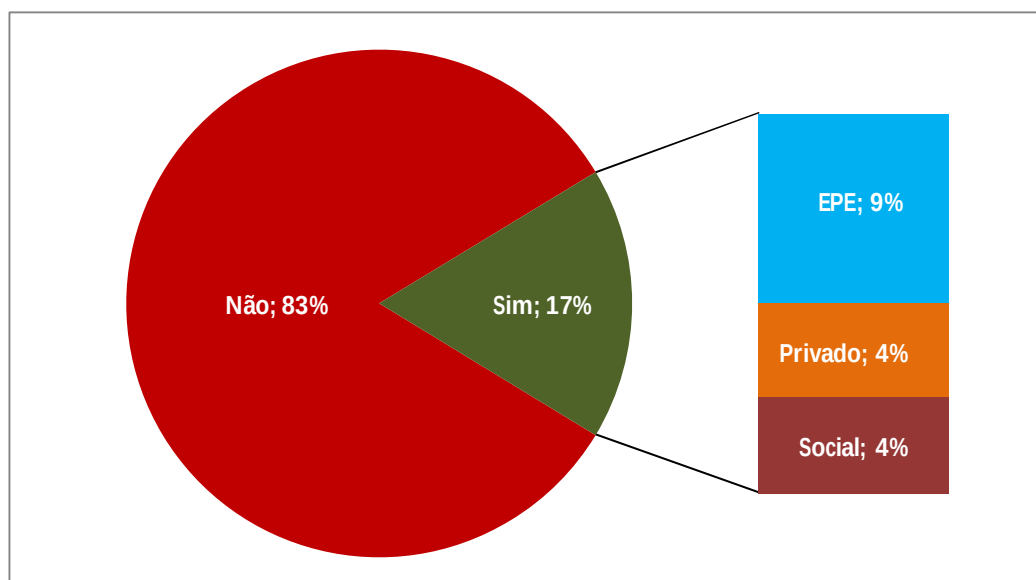


Figura 21 - Implementação de um Plano de Continuidade

Para os hospitais com implementação do *BCP* procurou-se aferir alguns indicadores que evidenciassem o grau de envolvimento da organização e a aplicação da metodologia indicada na construção de um plano.

- Alocação de recursos humanos e natureza da equipa envolvida:

Tabela 18 - Recursos Técnicos envolvidos e sua natureza

|             | 1-2        | 3-5                       | 5-10                      | > 10                                      |
|-------------|------------|---------------------------|---------------------------|-------------------------------------------|
| Privado     | Não refere |                           | Equipa Técnica Hospitalar |                                           |
| Público EPE |            |                           | Equipa Técnica Hospitalar | Equipa Técnica Hospitalar<br>Equipa Mista |
| Social      |            | Equipa Técnica Hospitalar | Equipa Técnica Hospitalar |                                           |

- Regularidade dos testes do Plano de Continuidade:
  - o Com regularidade:
    - § Semestral: 43%
    - § Anual: 29%
  - o Sem regularidade definida: 29%
- Incluem a Formação e Sensibilização dos Colaboradores no *BCP*:
  - o Não: 29%
  - o Sim: 71%
- Qual a periodicidade na preparação e manutenção do *BCP*:
  - o Mensal: 14%
  - o Trimestral: 29%
  - o Anual: 14%
  - o Trienal: 14%
  - o Nenhuma: 14%
  - o Sem Resposta: 14%
- Dias dispendidos na preparação e manutenção do *BCP*
  - o 30: 25%
  - o 15: 13%
  - o Sem resposta: 63%
- Responsabilidade pelo *BCP*:
  - o Administração: 63%
  - o Administração, Direcção SI e Equipa *BCP*: 13%
  - o Administração, Direcção Gestão do Risco: 13%
  - o Equipa *BCP*: 13%

Aos 83% dos hospitais que indicaram não ter implementado um *BCP*, 6% prevêm implementá-lo em 2010, 21% em 2011, 68% e 6% ou não têm planos definidos ou não responderam, respectivamente. Segmentando as respostas pela natureza do hospital, verifica-se que:

Tabela 19 - Previsão de Implementação de um *BCP*

|               | 2010 | 2011 | Não Definido | Sem Resposta |
|---------------|------|------|--------------|--------------|
| Social        | 67%  |      | 33%          |              |
| Privado       | 17%  | 33%  | 17%          | 33%          |
| Público Outro |      |      | 100%         |              |
| Privado       | 20%  | 30%  | 20%          | 30%          |
| Total         | 6%   | 21%  | 68%          | 6%           |

Quanto às causas que determinaram o adiamento desta iniciativa, estão distribuídas da seguinte forma:

Tabela 20 - Justificação do adiamento da decisão

|               | Alteração do paradigma hospitalar | Montante do Investimento | Outras prioridades | Recursos Técnicos | Sem resposta |
|---------------|-----------------------------------|--------------------------|--------------------|-------------------|--------------|
| Privado       |                                   | 13%                      | 53%                |                   | 33%          |
| Social        |                                   |                          | 50%                | 50%               |              |
| Público EPE   |                                   | 20%                      | 40%                | 7%                | 33%          |
| Público Outro | 17%                               |                          | 50%                |                   | 33%          |

A análise de impacto no negócio (*BIA – Business Impact Analysis*) é uma das peças essenciais na definição e construção de um plano de continuidade. Do conjunto das respostas verifica-se que 85% dos hospitais não dispõem de uma *BIA* (78%) ou não responderam (7%). Entre os hospitais que afirmam ter implementado um *BCP*, 75% não elaborou a respectiva *BIA* como suporte à análise no desenvolvimento do plano. Segmentando as respostas pelos diversos hospitais obtemos os seguintes resultados:

Tabela 21 - Análise de Impacto no Negócio

|             | Sim | Não  | N/R |
|-------------|-----|------|-----|
| Privado     | 13% | 75%  | 13% |
| Social      |     | 100% |     |
| Público EPE | 28% | 72%  |     |
| Total       | 15% | 78%  | 7%  |

Dos hospitais que elaboraram a *BIA*, 57% fizeram-no cobrindo a totalidade dos departamentos e processos de negócio do hospital. A *BIA* é somente utilizada na implementação da política de continuidade em 43% dos hospitais e em igual proporção é revista anualmente. Os restantes hospitais não têm planeada a revisão regular da *BIA*.

#### 4.8 Plano de Recuperação dos Desastres

Este subcapítulo procura identificar o grau de implementação de um Plano de Recuperação de Desastres – *DRP* – e qual a política de segurança dos dados.

Em 78% dos hospitais não existe este plano. Esta realidade é particularmente acentuada nos hospitais privados e outros hospitais públicos, que revelaram em 94% e 83%, respectivamente, não dispor de tal plano. Para os demais hospitais, a resposta negativa sobre a existência de uma política integrada de recuperação da informação em caso de desastre é, ainda assim, maioritária.

Tabela 22 – Existência de *DRP*

|         | Sim | Não |
|---------|-----|-----|
| Privado | 6%  | 94% |
| Social  | 40% | 60% |
| EPE     | 33% | 67% |
| Outro   | 17% | 83% |
| Total   | 22% | 78% |

O hospitais que indicaram dispor de um *DRP* efectuam a sua revisão com uma periodicidade:

Tabela 23 - Periodicidade na revisão do *DRP*

|         | Semestral | Anual | Não definida |
|---------|-----------|-------|--------------|
| Privado |           | 100%  |              |
| Social  | 50%       | 50%   |              |
| EPE     | 17%       | 66%   | 17%          |
| Outro   |           | 100%  |              |
| Total   | 70%       | 20%   | 10%          |

e incluem as fases de:

- o Teste, Auditoria e Manutenção: 30%
- o Auditoria e Manutenção: 20%
- o Teste: 20%
- o Manutenção: 20%
- o Não responderam: 10%

Relativamente aos resultados definidos no *DRP* e na Avaliação dos Riscos, 30% consideram-nos “bem definidos”, 50% “definidos minimamente”, 10% “pouco definidos” e 10% “mal definidos”.

#### 4.8.1 Políticas de segurança da informação digital

As políticas de salvaguarda da informação digital estão, há longa data, incorporadas nas boas práticas das organizações. Em 98% dos hospitais existe a prática regular de *backup* da informação. Esmiuçando as respostas, obtemos os seguintes quadros de análise:

Tabela 24 - Periodicidade dos Backups

|              | Contínua | Horária | Diária | Semanal | Não definida |
|--------------|----------|---------|--------|---------|--------------|
| Privado      |          | 13%     | 87%    |         |              |
| Social       | 20%      |         | 60%    |         | 20%          |
| EPE          | 6%       |         | 88%    | 6%      |              |
| Outro        | 17%      |         | 83%    |         |              |
| Não definido |          |         | 100%   |         |              |
| <b>Total</b> | 7%       | 4%      | 85%    | 2%      | 2%           |

A periodicidade diária é a modalidade utilizada por 85% dos inquiridos, sendo que alguns hospitais seguem a política de *backup* em contínuo (*mirroring*) com um backup total diário. Relativamente à confiabilidade dos *backups*, validada pelos procedimentos de recuperação, 97% dos hospitais consideram-na “Muito Confiável” (35%) ou “Confiável” (61%). Esta realidade é atestada pela assertividade de 96% dos hospitais que afirmam dispor de um sistema de *backup* e de recuperação de dados, bem assim como de 81% dos hospitais que admitem ter nos seus recursos humanos, técnicos habilitados a reagir imediatamente em caso de falha.

Tabela 25 – Confiabilidade dos Backups e Procedimentos de Recuperação

|              | Muito Confiáveis | Confiáveis | Não definida |
|--------------|------------------|------------|--------------|
| Privado      | 38%              | 62%        |              |
| Social       | 20%              | 60%        | 20%          |
| EPE          | 39%              | 61%        |              |
| Outro        | 33%              | 50%        | 17%          |
| Não definido |                  | 100%       |              |
| <b>Total</b> | 35%              | 61%        | 4%           |

Como nota final relativamente à política de segurança, importa realçar o facto de 59% dos hospitais referirem que os suportes físicos aos *backups* se encontram no mesmo espaço físico do *datacenter*, não contribuindo para a minimização do risco associado a desastre no mesmo espaço. Quanto aos restantes 41%, que minimizam o risco conservando os *backups* em local diferente, as opções de deslocalização utilizadas são as seguintes:

Tabela 26 - Localização dos Backups

|                         |                                                            |
|-------------------------|------------------------------------------------------------|
| Cofre                   | Nos <i>Datacenters</i> de outras unidades do grupo         |
| No Hospital e Sede      | <i>Datacenter</i> e Bastidor deslocalizado noutra edifício |
| Armazenamento Externo   | Disco Externo                                              |
| No Hospital, fora do DC | CA Arcserv                                                 |

#### 4.9 Plano hospitalar de Emergência

A exigência legal de que as organizações disponham de um Plano de Emergência de Risco de Incêndio, estabelecida pelo Decreto-Lei n.º 220/2008, de 12 de Novembro, conforme apresentado no subcapítulo 1.4 -Gestão da Continuidade do Negócio no contexto hospitalar, não encontra eco em 16% dos hospitais inquiridos que afirmam que a organização não dispõe de um Plano de Emergência.

Dos restantes, 24% indica que o plano foi elaborado numa perspectiva interna, 4% numa perspectiva externa e 52% foi desenvolvido conjugando ambas as perspectivas.

Tabela 27 – Planos de Emergência: Existência e Perspectivas de desenvolvimento.

|              | Não | Sim     |         |       | Não Definido |
|--------------|-----|---------|---------|-------|--------------|
|              |     | Interna | Externa | Ambas |              |
| Privado      | 25% | 38%     | 0%      | 31%   | 6%           |
| Social       | 40% |         |         | 60%   |              |
| EPE          |     | 11%     | 6%      | 77%   | 6%           |
| Outro        | 17% | 49%     | 17%     | 17%   |              |
| Não definido |     |         |         | 100%  |              |
| Total        | 16% | 24%     | 4%      | 52%   | 4%           |

O teste dos planos é uma actividade integrada no processo de melhoria contínua de uma organização. Desde a validação de procedimentos e protocolos estabelecidos à promoção da resiliência da organização face à adversidade, o exercício de simulacros íntegra o ciclo de gestão da emergência no hospital. Para 49% dos hospitais esta prática ainda não está instituída, pois referem não ter regularidade na execução de simulacros. Entre os que admitem essa prática regular, 41% definiram a promoção de simulacros anualmente.

Tabela 28 - Regularidade nos Testes dos Planos de Emergência

|              | Mensal | Semestral | Anual | Bianual | Não definida |
|--------------|--------|-----------|-------|---------|--------------|
| Privado      |        |           | 45%   |         | 55%          |
| Social       |        |           | 67%   |         | 33%          |
| EPE          | 6%     | 6%        | 24%   | 12%     | 52%          |
| Outro        |        |           | 80%   |         | 20%          |
| Não definido |        |           |       |         | 100%         |
| Total        | 3%     | 3%        | 41%   | 5%      | 48%          |



## 5 Metodologia aplicada no desenvolvimento de um plano de continuidade

Paralelamente à pesquisa efectuada e cujos resultados foram apresentados no capítulo anterior, desenvolveu-se um caso de estudo num hospital, com o objectivo de validar uma abordagem metodológica no desenvolvimento de um Plano de Continuidade do Negócio (BCP), que envolvesse a organização no processo de levantamento de processos e identificação dos riscos, utilizando instrumentos criativos na abordagem. O âmbito de desenvolvimento da metodologia circunscreveu-se aos processos suportados por TICs.

Este capítulo apresenta as várias propostas metodológicas existentes, emanadas de institutos de conformidade e a metodologia que foi aplicada no serviço hospitalar em estudo.

### 5.1 Os standards internacionais para a Gestão da Continuidade do Negócio

A política de Gestão da Continuidade do Negócio, tal como outras políticas de gestão do risco, é tanto ou mais eficaz quanto fundamentada em normas internacionalmente aceites e elaboradas de acordo com os objectivos do negócio. Este enquadramento da BCM nos objectivos do negócio e nos standards internacionalmente aceites conferem credibilidade e viabilidade a um programa de continuidade. Neste subcapítulo apresenta-se uma súmula das propostas metodológicas de cada instituto internacional que se dedica a definir as boas práticas desta temática.

De acordo com Hiles (Hiles 2007), antes de 11 de Setembro de 2001, havia cerca de vinte standards internacionais, que proliferaram após a fatídica data. Hoje ultrapassam as quatro dezenas (Anexo C). De realçar a massiva presença de organizações integrantes do universo de países anglo-saxónicos ou com forte influência cultural deste universo.

Para além da sucessão de eventos imprevisíveis, como o referido, que introduziram a temática nas preocupações de sustentabilidade das organizações, o papel do regulador na produção de orientações é também um factor determinante. A publicação do *Civil Contingency Act 2004* do Reino Unido, que entrou em vigor em 2006, foi determinante na proliferação de iniciativas em prol da Continuidade das organizações (Hiles 2007).

Na síntese que a seguir se apresenta, destacam-se aqueles que se consideram mais relevantes como referenciais de boas práticas.

#### 5.1.1 Disaster Recovery Institute International – DRII

O *Disaster Recovery Institute International (DRII)* foi fundado em 1988 nos Estados Unidos da América com o “objectivo de desenvolver um repositório de conhecimento em planeamento da contingência e gestão do risco” (DRII). Hoje ocupa o primeiro lugar como instituto de formação e certificação na área do BCM.

A metodologia proposta pelo DRII, sem qualquer ordem de importância ou de sequência, é composta por 7 fases (DRII):

1. **Iniciação do Programa/Projecto de Continuidade**, com o objectivo de definir as necessidades de um programa de BCM com:
  - i. Estratégias de Resiliência,
  - ii. Objectivos de Recuperação,

- iii. Suporte da Administração,
  - iv. Gestão do Risco Operacional,
  - v. Planos de Gestão de Crise;
2. **Controlo e Avaliação do Risco**, com o objectivo de determinar os riscos que possam afectar a organização e os seus recursos – pessoas, instalações e tecnologias – e as potenciais perdas para o negócio, bem assim como os controlos necessários para mitigar os seus efeitos.
  3. **Análise de Impacto no Negócio**, com o objectivo de identificar os impactos resultantes das interrupções que possam afectar o negócio e as técnicas que podem ser utilizadas para quantificar e qualificar esses impactos.
  4. **Estratégias de Continuidade do Negócio**, com o objectivo de alavancar a Análise de Impacto do Negócio e o Controlo e Avaliação do Risco e recomendar estratégias de continuidade. A base destas estratégias é o objectivo de *Recovery Time* e de *Recovery Point*.
  5. **Operações e Resposta de Emergência**, com o objectivo de identificar a prontidão das organizações na resposta a situações de emergência de forma coordenada, oportuna e eficaz e desenvolver procedimentos de resposta inicial e estabilização da situação de crise.
  6. **Plano de Continuidade do Negócio**, com o objectivo de projectar, desenvolver e implementar Planos de Continuidade de Negócios que promovam a continuidade e/ou recuperação, identificados pelos requisitos da organização.
  7. **Programas de Sensibilização e Formação**, com o objectivo de criar e manter a sensibilização da organização e reforçar as competências necessárias para desenvolver e implementar a *BCM*.
  8. **Exercícios, Auditoria e Manutenção do Plano de Continuidade**, com o objectivo de estabelecer um programa que documente as necessidades de exercícios, incluindo o planeamento, programação, comunicação, auditoria e revisão do plano, um programa de auditoria que valide a conformidade com os standards mais actuais e um programa de manutenção que mantenha o plano actual, adequado e completo.
  9. **Relações Públicas e Coordenação da Crise**, com o objectivo de desenvolver e documentar os planos de acção de comunicação das informações. Coordenar e exercitar com os interessados e os *média* de forma a garantir a clareza na comunicação de crise.
  10. **Coordenação com as Autoridades**, com o objectivo de estabelecer os procedimentos e políticas de coordenação com autoridades intervenientes, de forma a garantir a sua conformidade com os dispositivos legais existentes.

#### 5.1.2 *British Standard Institute – BSI*

Fundado em 1901 como *Engineering Standards Committee*, o BSI Group tornou-se uma referência internacional na elaboração de standards, sendo actualmente o *National Standards Body* do Reino Unido (BSI). Entre os diversos standards encontra-se a norma BS25999 inteiramente dedicada ao *BCM*.

A norma BS2599 estabelece as bases para a compreensão, desenvolvimento e implementação da continuidade do negócio dentro da organização e integra disciplinas como a gestão do risco

e de processos, com a continuidade do negócio, promovendo a confiança entre empresas e seus clientes. É composta por dois documentos:

- BS25999-1: *Code of Practice* – Descreve os objectivos gerais da norma, orientação e recomendações. Esta parte descreve as “boas práticas”, estando para além de um conjunto mínimo de requisitos e analisa as oportunidades de gestão de risco e os métodos para obtenção dos objectivos do negócio;
- BS25999-2: *The Specification* – Descreve o detalhe das actividades que têm de ser descritas de forma a atingir os objectivos de continuidade do negócio definidos pela filosofia de gestão da organização. Define os requisitos de objectivos mínimos para um eficaz Sistema de BCM e fornece um enquadramento para a sua implementação, gestão e melhoria contínua.

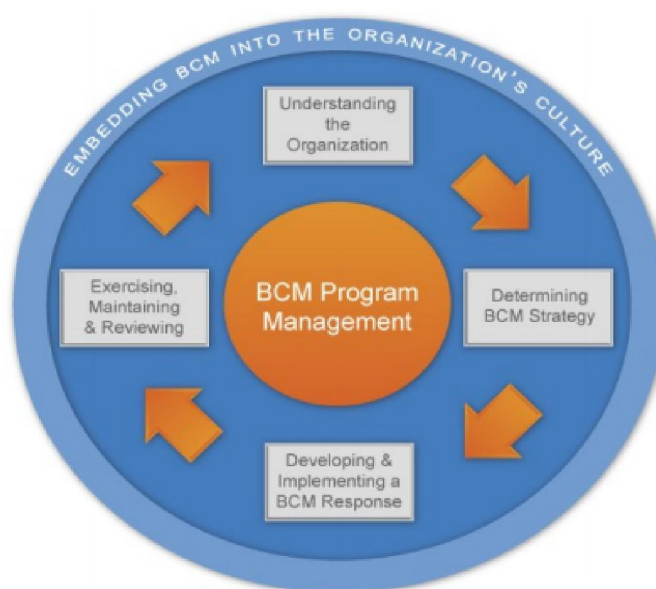


Figura 22 – BSI2599 BCM Program (BSI)

A BS25999 é uma norma internacionalmente aceite, orientada para a focalização das questões chave definidas para aumentar a capacidade de resposta, resiliência e recuperação da organização.

Esta norma não foi desenvolvida especificamente para nenhuma indústria ou empresa, antes fornece uma base para qualquer organização que reconheça a necessidade de um Sistema de BCM.

Os benefícios decorrentes, por si só, valem o esforço de desenvolvimento e implementação de um Sistema de BCM. Qualquer incidente que prejudique a capacidade da empresa funcionar pode impactar negativamente a organização, mesmo depois de retomar a normalidade das operações.

O ciclo de vida na Gestão de Continuidade de Negócio (*Business Continuity Management Lifecycle*) tal como definido por esta entidade, é composto por seis etapas (Figura 22):

- Gestão do Programa de Continuidade;
- Identificação das necessidades da Organização;

- Definição das Estratégias de Continuidade;
- Desenvolvimento e implementação do(s) Plano(s);
- Ensaio, manutenção e revisão dos Planos de Continuidade;
- Incorporar a Continuidade na cultura da Organização.

A parte 2 – *Specification* – está organizada em quatro fases e por um conjunto de actividades em cada fase. A Tabela 29 apresenta as fases do Sistema de BCM e elenca as actividades a desenvolver em cada uma delas.

Tabela 29 – BS25999-2 Fases e Actividades do Sistema de BCM (BSI)

| Fase       | Planeamento do Programa de BCM                                                                                                                                                                                           | Implementação e Operação do Programa                                                                                                                                                                                                                                                                                 | Monitorização e Análise do Programa                                                      | Manutenção e Melhoria do Programa                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Actividade | <ul style="list-style-type: none"> <li>• Requisitos do Programa</li> <li>• Política de BCM</li> <li>• Definição dos recursos e competências</li> <li>• Incorporação do BCM</li> <li>• Documentação e Registos</li> </ul> | <ul style="list-style-type: none"> <li>• Análise do Impacto no Negócio</li> <li>• Avaliação dos Riscos</li> <li>• Determinação da Escolhas</li> <li>• Estrutura de Resposta aos Incidentes</li> <li>• Planos de Emergência e de Continuidade</li> <li>• Exercícios</li> <li>• Manutenção e Revisão do BCM</li> </ul> | <ul style="list-style-type: none"> <li>• Auditoria Interna</li> <li>• Revisão</li> </ul> | <ul style="list-style-type: none"> <li>• Acções Preventivas e Correctivas</li> </ul> |

### 5.1.3 IT Information Library – ITIL

No início da década de 80, o governo inglês, através da OCG (*Office of Government Commerce*) produziu um conjunto de livros com boas práticas na gestão de serviços em TI. Esta iniciativa deu origem ao ITIL (*IT Infrastructure Libray*), uma biblioteca de boas práticas. O sucesso desta iniciativa tem levado a uma contínua melhoria do conceito que hoje deixou de estar confinado à gestão de serviços de TI e se alargou à Gestão de Serviços assente no ciclo de vida do produto. Actualmente, esta biblioteca vai na versão 3 e é composta por cinco livros e um guia introdutório:

- *Introduction to ITIL Service Management Practices*,
- *Service Strategy*;
- *Service Design*;
- *Service Transition*;
- *Service Operation*;
- *Continual Service Improvement*;

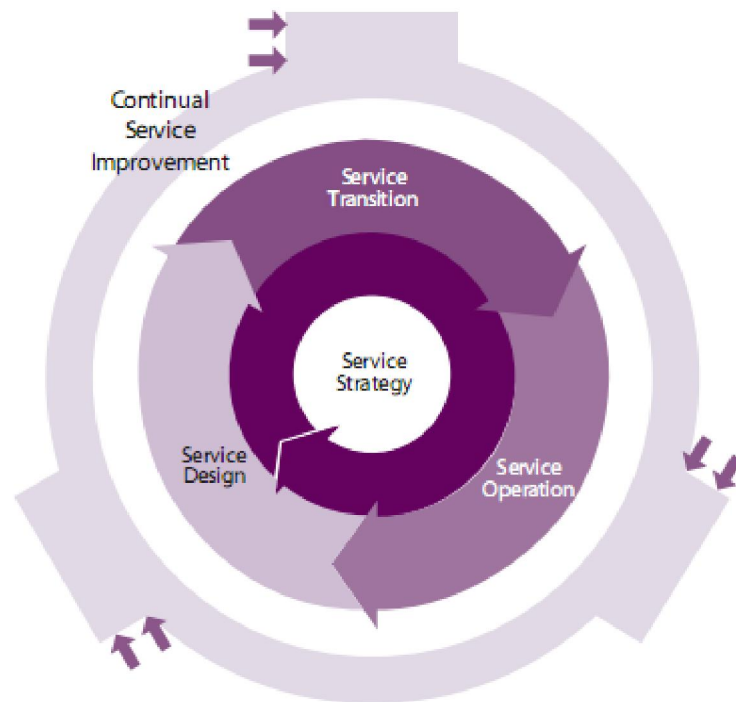


Figura 23 - Biblioteca ITIL (ITIL)

O livro *Service Design* é dedicado às boas práticas no desenho e desenvolvimento de serviços e processos de gestão de serviços, seja para novos serviços seja para serviços já implementados. Os processos decorrentes do *Service Design* são (ITIL):

- *Service Catalogue Management*
- *Service Level Management*
- *Capacity Management*
- *Availability Management*
- ***IT Service Continuity Management (ITSCM)***
- *Information Security Management*
- *Supplier Management*

O processo ITSCM comporta a metodologia a aplicar no desenvolvimento de um *BCP* que se caracteriza pelas seguintes etapas (Figura 24):

1. **Iniciação:** cobre toda a organização e é composta pelas seguintes actividades:
  - a. Definição das Políticas;
  - b. Especificação dos termos de referência e âmbito;
  - c. Alocação de recursos humanos e financeiros;
  - d. Definição da estrutura de organização e controlo do projecto;
  - e. Definição dos *deliverables* e da qualidade dos planos;

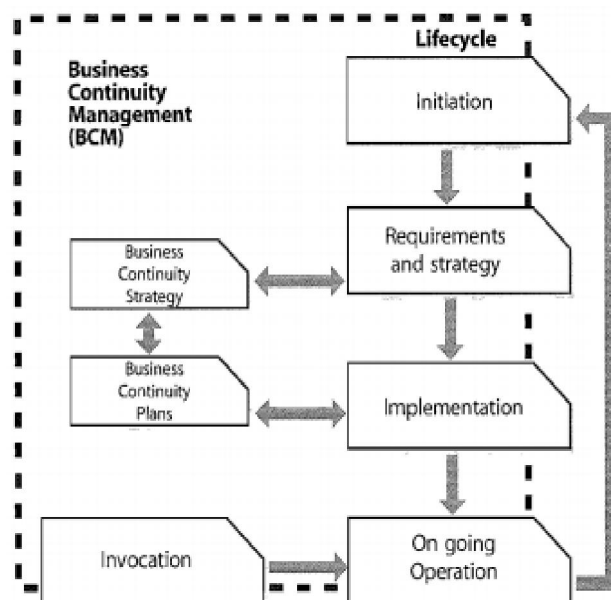


Figura 24 - Metodologia ITSCM (ITIL)

2. **Requisitos e estratégia:** definição dos requisitos do negócio necessários para a sua continuidade e de como a organização sobreviverá a uma disrupção e quais os custos que poderão incorrer.
  - a. Requisitos:
    - i. Análise de Impacto do Negócio;
    - ii. Avaliação do Risco;
  - b. Estratégia:
    - i. Documentar as medidas de redução do risco identificadas nos requisitos e os processos de recuperação do negócio.
3. **Implementação:** Desenvolvimento dos *IT Service Continuity Plans* em conformidade com o *BCP*. Os planos de ITSCM devem ser desenvolvidos de forma a disponibilizar a informação necessária para os sistemas críticos, serviços e instalações de forma a manterem a entrega de serviço num tempo aceitável. Os ITSCM *Plans* são mais do que planos de recuperação e devem endereçar todas as actividades necessárias para garantir que os sistemas, serviços e recursos são disponibilizados num estado operacional aceitável e adequados para o propósito. Para além do ITSCM *Plan*, devem ser produzidos um conjunto de planos integrados com o *BCP*:
  - a. Plano de Resposta de Emergência;
  - b. Plano de Avaliação dos Danos;
  - c. Plano de Salvamento;
  - d. Plano de Registos Vitais;
  - e. Plano de Relações Públicas e de Gestão da Crise;
  - f. Plano de Serviços de Alojamento;
  - g. Plano de Segurança;
  - h. Plano do Pessoal;
  - i. Plano de Comunicações;
  - j. Plano de Administração e Finanças;
4. **Operações Contínuas:** Esta fase é composta pelas seguintes actividades:
  - a. Sensibilização, Educação e Formação;

- b. Revisão;
- c. Teste;
- d. Gestão de Alterações;
- e. Invocação: último teste de garantia de que os planos são adequados e estão devidamente alinhados entre si.

#### 5.1.4 Control Objectives for Information and related Technology – COBIT

A metodologia COBIT – *Control Objectives for Information and related Technology* é uma *framework* que fornece as melhores práticas para a gestão de processos de TI, estruturados de uma forma lógica, atendendo as várias necessidades de gestão da organização, tratando os riscos de negócio, questões técnicas, necessidades de controlo e métricas de desempenho. O COBIT não é um padrão definitivo, ele serve como apoio para a implementação de controlos na Governança de TI. (ITGI 2007)

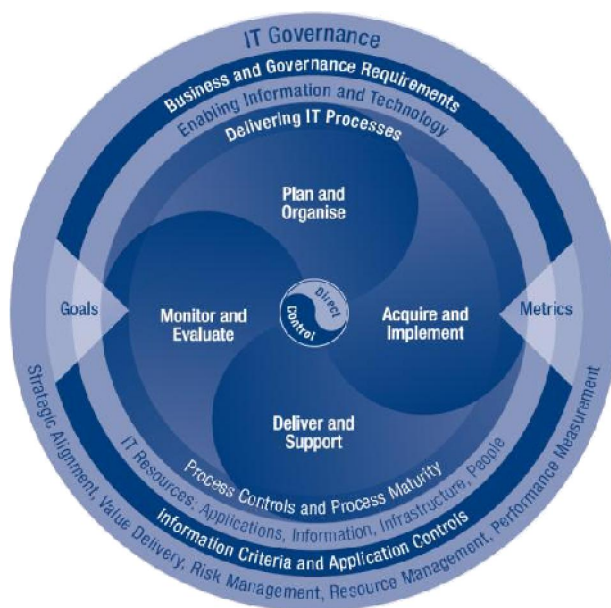


Figura 25 - COBIT 4.1

Nesta metodologia os Processos de TI estão organizados em:

- **4 Domínios:**
  1. **Planeamento e Organização;**
  2. **Aquisição e Implementação;**
  3. **Entrega e Suporte;**
  4. **Monitorização e Avaliação;**
- **34 Processos:**
- **214 Objectivos de Controlo**

A metodologia específica aplicada à continuidade enquadra-se no domínio de **Entrega e Suporte**. Este domínio preocupa-se com as entregas reais dos serviços requeridos, que abrangem as operações tradicionais sobre aspectos de segurança e continuidade, até à formação. As actividades concernentes à continuidade do negócio estão suportadas pelo processo **DS4 – Gerir a Continuidade dos Serviços** que a seguir se descreve sucintamente (Brand and Boonen 2004):

1. Definição dos Requisitos e da Estratégia de Continuidade das TI;
2. Execução da Avaliação de Risco;
3. Desenvolvimento e Manutenção do *BCP* das TI;
4. Teste e Implementação do *BCP* das TI;
5. Criação e Manutenção de Planos e Procedimentos de Recuperação;
6. Educação e Formação de utilizadores e gestores;
7. Avaliação do *BCP*;
8. Monitorização do Processo.

Os objectivos de controlo definidos para este processo são os seguintes:

- DS4.1 – *Framework* de Continuidade das TI;
- DS4.2 – Planos de Continuidade de TI;
- DS4.3 – Recursos Críticos de TI;
- DS4.5 – Manutenção do Plano de Continuidade de TI;
- DS4.6 – Teste do Plano de Continuidade de TI;
- DS4.7 – Distribuição do Plano de Continuidade de TI;
- DS4.8 – Recuperação e Retoma de Serviços TI;
- DS4.9 – Alojamento dos Backups *Offsite*;
- DS4.10 – Revisão da Pós-retoma;

## 5.2 Caracterização do serviço hospitalar

O caso de estudo foi desenvolvido no Hospital da Prelada Dr. Domingos Braga da Cruz (HP), integrado na rede de hospitais do sistema social e pertencente à Santa Casa da Misericórdia do Porto. O HP iniciou a actividade em Outubro de 1988 e presta serviços de saúde nas valências de (SCMP 2010):

- v Anestesiologia
- v Cirurgia Geral e Urologia
- v Cirurgia Plástica e Reconstructiva e Unidade de Queimados
- v Ortopedia
- v Ambulatório
- v Medicina Física e de Reabilitação
- v Meios Complementares de Diagnóstico e Tratamento
- v Oftalmologia

Em 2007, o HP recebeu do Organismo Internacional de Acreditação, o *Health Quality Service* (HQS), a **Acreditação Total em Qualidade**, referente a todas as áreas do Hospital, sendo o primeiro Hospital privado em Portugal a receber a Acreditação em Qualidade, por um

organismo nacional ou internacional, tendo sido auditado em todas as áreas de actividade do Hospital desde a Gestão, Serviços Clínicos, Serviços Não Clínicos, Serviços de Apoio e Administrativos.

### 5.2.1 Missão, Visão e Valores

- **Missão**

Melhorar a saúde através de cuidados de qualidade, garantindo acesso atempado e a optimização dos recursos disponíveis na comunidade, assim como participar na investigação e no ensino pós-graduado.

- **Visão**

Pelo seu posicionamento (socialmente responsável, promotora da equidade de acesso, não lucrativa) e pela excelência dos resultados obtidos nas diversas especialidades de que dispuser, o Hospital será reconhecido – pela comunidade, pelo S.N.S. e pelos restantes interessados – como um Estabelecimento de qualidade na saúde, tanto pelos cuidados prestados como pela sua participação na investigação e no ensino pós-graduado.

- **Valores**

- v Servir o doente;
- v Excelência de actuação;
- v Respeito e correcção no relacionamento;
- v Valor para a comunidade;
- v Inovação para melhores serviços e resultados;
- v Responsabilidade por tudo o que fazemos.

### 5.2.2 Estrutura Organizacional

O HP pertence à Santa Casa da Misericórdia do Porto (SCMP), uma instituição de caridade e assistência social, de fins filantrópicos e de utilidade pública, que foi fundada em 14 de Março de 1499. Actualmente a acção assistencial da Misericórdia do Porto, diversifica-se em algumas áreas muito importantes: terceira-idade, **saúde**, deficiência, pobreza e exclusão social, habitação, cultura, ensino e formação profissional, lazer, etc.

O órgão gestor da SCMP é a Mesa Administrativa, composta por treze elementos em regime de voluntariado, a quem está cometida a responsabilidade de supervisionar as diversas unidades organizacionais que compõem a acção assistencial da SCMP, entre elas o HP.

A estrutura organizacional do HP (Anexo D) é composta por um Conselho de Gerência que administra as actividades clínicas e de suporte. A matriz organizacional do HP segue um modelo de organização misto, com áreas delimitadas pela função interna, mas agregando as várias funções em áreas de prestação de serviço, como por exemplo a Área de Prestação de Cuidados, que incorpora as diversas valências clínicas e as unidades de apoio clínico,

### 5.2.3 Modelo de Negócio

A prestação de cuidados de saúde é efectuada por um conjunto diversificado de actores que, em rede, criam a oferta de cuidados de saúde, configurando uma constelação de valor (Normann and Ramírez 1993).

A figura 26 representa a constelação de valor em que a “estrela de valor” é o “doente/utente/cliente”, conforme a nomenclatura adaptada a cada uma das relações. Para satisfazer a sua procura de cuidados de saúde, o “Cliente/Utente/Doente” dispõe de uma multiplicidade de prestadores de serviços de saúde. É nesta rede de valor que o HP está inserido e estão representadas as diversas relações para providenciar os cuidados de saúde.

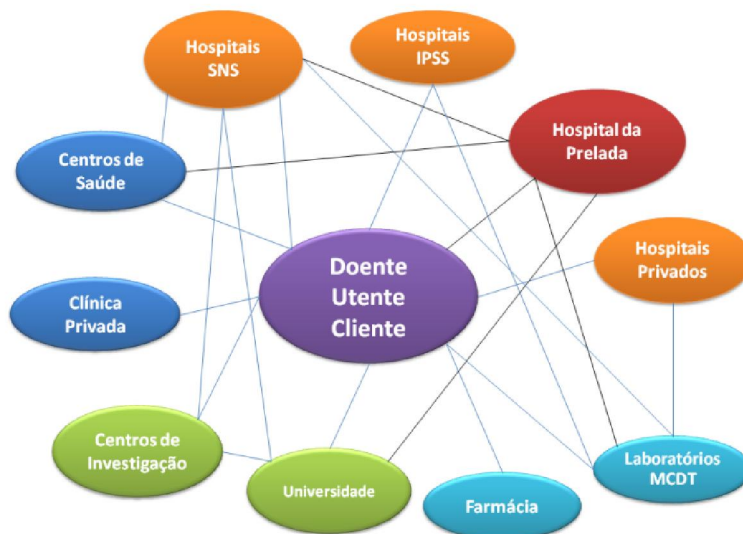


Figura 26 - Constelação de Valor dos Cuidados de Saúde

A prestação de serviços médico – cirúrgicos do HP é destinada aos utentes do Serviço Nacional de Saúde (80%), outros subsistemas de saúde (ADSE, ADME, SEGUROS) (16%) e integra nas suas instalações uma unidade de consulta privada (4%), a quem fornece serviços de suporte à cirurgia e internamento. Os serviços de diagnóstico estão externalizados a um laboratório da especialidade que partilha a infra-estrutura do HP.

Relativamente às Áreas de Negócio, os proveitos do HP estão distribuídos por Consulta Externa (20%), Meios Complementares de Diagnóstico (Análises Clínicas e Hemoterapia) e Tratamento (Medicina Física e Reabilitação) (4%) e Cirurgia (Acto Cirúrgico e Internamento) (76%).

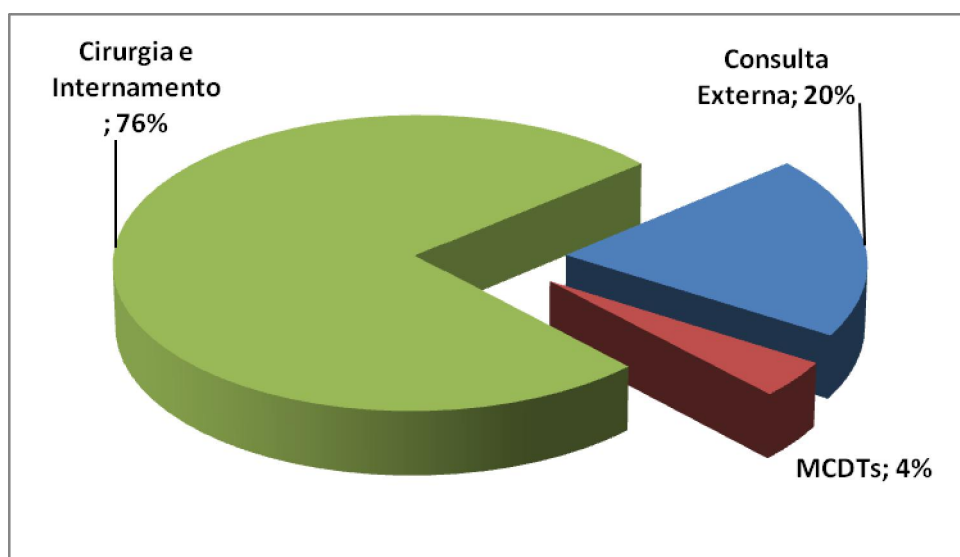


Figura 27 - Principais Áreas de Negócio do HP

Do conjunto de actividades, o HP tem parcerias com Clínicas, Laboratório de Imagiologia e o Centro Renal, e externalizou os serviços de Lavandaria, Alimentação, Bar, Segurança, Limpeza e Jardinagem. Os restantes serviços são efectuados por colaboradores do HP.

### 5.3 Âmbito de aplicação da metodologia

O caso de estudo desenvolvido no Hospital da Prelada circunscreveu-se aos processos de negócio suportados pelas TICs e foram efectuadas as primeiras quatro fases da metodologia a seguir aplicada. Relativamente às fases subsequentes, fica uma descrição conceptual dos seus objectivos e componentes específicos.

### 5.4 Metodologia aplicada no desenvolvimento do plano

As propostas metodológicas no desenvolvimento de um *BCP* variam de acordo com o instituto promotor, conforme descrito no capítulo 2.5. O processo metodológico seguido na elaboração do *BCP* é composto de seis fases:



Figura 28 - As fases de desenvolvimento do BCP

#### 5.4.1 Governança

A palavra Governança é um derivado do verbo “governar”. De acordo com o Dicionário de Língua Portuguesa da Texto Editora, o verbo governar tem um variado conjunto de significados, entre eles: reger, administrar, gerir, dominar, imperar sobre; mandar, exercer autoridade, administração, governo, regular-se, ...; Importa, no entanto, realçar que a palavra “governo” é uma palavra derivada da expressão grega *kubernan*, que significa “dirigir”.

Governança não é um conceito novo. Usado há muito tempo na administração, o termo tornou-se uma categoria analítica, associada a conceitos como participação, parceria,

aprendizagem colectiva, regulação, e práticas de bom governo, como orçamento participativo e acções de desenvolvimento local e regional. Em TI, este conceito tem servido de “guarda-chuva” para uma lista de acrónimos. Entre eles, se destacam ITIL, COBIT e CMMI.

A perspectiva holística que se defende na abordagem de uma política de continuidade e sustentabilidade da organização, confere a esta abordagem um particular destaque no envolvimento da administração ao mais alto nível no processo. A dimensão estratégica desta política, geradora de vantagens competitivas e contribuinte efectiva da preservação de valor, enquadra-se no *core* de preocupações da administração de uma organização. Por outro lado, a transversalidade desta política determina a alocação de recursos humanos e financeiros que somente podem ser garantidos pela administração da organização.

De acordo com o Gartner Group, um plano efectivo de *BCM* requer o envolvimento de todas as linhas de negócio e de todos os níveis de gestão (Witty and Stevens 2010). A percepção comum de que esta política se enquadra nas actividades da Direcção de Sistemas de Informação é redutora e ausente da perspectiva holística que se defende. A tabela 30 apresenta as causas e consequências da ausência de envolvimento da administração e outros níveis de direcção na elaboração de um *BCP*.

Tabela 30 - Causas e Consequências da Falta de Suporte no Programa de BCP

| Problema                         | Causa                                                                                                                                                                      | Consequência                                                                                                                                                                                                                                                                                       |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sem Suporte da Gestão Executiva  | <ul style="list-style-type: none"><li>• Não há percepção do risco</li><li>• Não vêem o valor para o negócio</li><li>• Consideram a <i>BCM</i> um assunto das TIC</li></ul> | <ul style="list-style-type: none"><li>• Falta de recursos financeiros</li><li>• Não há boa vontade para alterar os processos e promover a resiliência</li><li>• Pouco apoio da gestão do negócio</li><li>• Baixa probabilidade de aplicar um programa de <i>BCM</i> sustentável</li></ul>          |
| Sem Suporte da Gestão do Negócio | <ul style="list-style-type: none"><li>• Todas as referidas acima</li><li>• Não há suporte da gestão de topo</li><li>• Colaboração e Comunicação inadequadas</li></ul>      | <ul style="list-style-type: none"><li>• Falta de envolvimento e suporte no planeamento dos processos, incluindo a sensibilização, formação, desenvolvimento, exercícios e revisão</li><li>• Validação inadequada dos <i>inputs</i> e planos</li><li>• Falta de suporte dos profissionais</li></ul> |
| Sem Suporte do Profissionais     | <ul style="list-style-type: none"><li>• Todas as referidas acima</li><li>• Não há suporte da gestão do negócio</li></ul>                                                   | <ul style="list-style-type: none"><li>• Todas as referidas acima</li><li>• Os planos não são desenvolvidos nem actualizados</li><li>• Ninguém aparece nos testes de recuperação</li></ul>                                                                                                          |

Fonte: Adaptado de Gartner Research (Witty and Stevens 2010)

Pese embora o âmbito deste caso de estudo, procurou-se envolver a administração e demais quadros dirigentes dos sectores do HP, sensibilizando-os para esta temática, através da organização de uma *workshop* (Anexo I) sob o tema “Identificando riscos, construindo alternativas”. O primeiro objectivo consistiu na apresentação do estudo em curso e de toda a

temática à volta do tema, evidenciando-se a necessidade de envolvimento e sensibilização de toda a estrutura colaborativa do HP neste desiderato. Para além de uma apresentação expositiva da metodologia presente, foram efectuadas duas actividades de *team work* com o objectivo de realçar dois dos requisitos da continuidade:

1. Conhecer o papel de cada interveniente na actividade do HP e as relações de interdependência existente entre eles;
2. A acção conjunta na construção das soluções de continuidade e a perspectiva colaborativa como instrumento sinérgico com vista à continuidade;

#### **5.4.2 Programa de Acção**

Desde o princípio deve ser claro qual o âmbito, objectivos, metodologia, *timing* e o cronograma de acções a desenvolver (Cornish 2007). Assim, um programa de acção deve conter:

- Actividades chave a analisar e pessoas responsáveis;
- Definição dos *milestones* e *deliverables*;

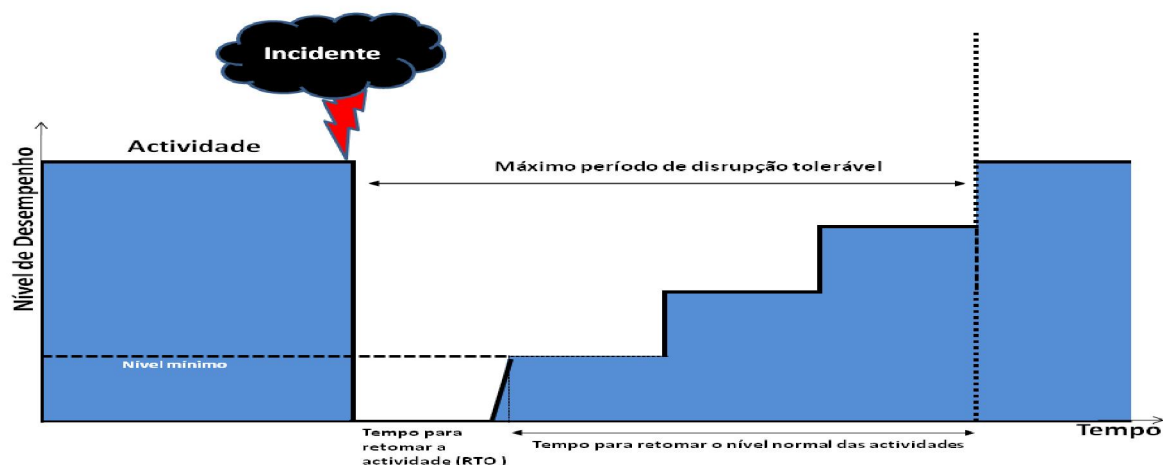
Neste pressuposto, foi elaborado um programa de entrevistas com os responsáveis das Áreas de Negócio identificadas – Consulta Externa, Admissão de Doentes e Cuidados Médico-Cirúrgicos – com o objectivo de identificar os processos de negócio e suas interdependências, com os responsáveis dos Sistemas de Informação, para identificar as várias aplicações e sistemas de suporte às operações descritas.

Numa segunda fase foram elaborados questionários para fundamentar a análise de impacto no negócio de cada um dos processos/linha de negócio.

#### **5.4.3 Análise do Impacto no Negócio**

A Análise de Impacto no Negócio (*Business Impact Analysis – BIA*) é uma das actividades fundamentais na construção do BCP. É uma análise ao nível da gestão que visa identificar a exposição da organização a perdas resultantes de uma súbita quebra das actividades do negócio ou de recursos de suporte, devidos a acidente, desastre e/ou ameaça. A BIA envolve a:

1. Identificação das actividades e sua interdependência, activos, infra-estrutura de suporte ou recursos que devam manter-se em continuidade ou recuperados ao longo do tempo;
2. Avaliar os impactos ao longo do tempo que ocorreriam se uma actividade sofresse uma interrupção;
3. Determinar o “Tempo Máximo do Período de Interrupção” de cada actividade, pela identificação do:
  - a. Máximo período de tempo após o início da interrupção no qual as actividades devam ser reassumidas;
  - b. O nível mínimo a que a actividade deve funcionar após o recomeço;
  - c. O período de tempo para que os níveis normais de actividade seja restabelecidos.



Adaptado de (Cornish 2007)

Figura 29 - Máximo Período Tolerável de Disrupção.

### Identificação dos processos de negócio

É um princípio básico de uma organização, desenvolver a gestão dos seus processos internos e também a forma de comunicação destes processos com os seus fornecedores e parceiros de negócios, que podemos chamar de processos externos à organização. Tal visa identificar as interfaces entre esses processos, as responsabilidades das áreas da empresa, das pessoas e o desempenho esperado, medido por indicadores e metas. Além disso, para uma empresa de serviços, existem dois elos na cadeia de relacionamento que são os clientes e os fornecedores, não sendo possível à empresa dissociar seus processos da interacção com seus consumidores e parceiros de negócio.

A partir das entrevistas efectuadas com os diversos intervenientes e de um estudo de implementação do Sistema Integrado de Gestão de Inscritos para Cirurgia (SIGIC) conduzido pela Cláudia Lopes (Mestrado Integrado em Engenharia Industrial e Gestão Industrial), identificaram-se os seguintes processos de negócio:

Tabela 31 - Áreas e Processos de Negócio do HP

| ÁREAS DE<br>NEGÓCIO     | CONSULTA EXTERNA                                        | ADMISSÃO DE DOENTES                                                                  | CUIDADOS<br>MÉDICO-CIRÚRGICOS                                                       |
|-------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| PROCESSOS DE<br>NEGÓCIO | Pedir Consulta<br>Planear Consulta<br>Realizar Consulta | Pedir Cirurgia<br>Programar Cirurgia<br>Realizar Consulta e MCDT<br>Planear Cirurgia | Internar Doente<br>Realizar Cirurgia<br>Realizar Recobro<br>Convalescer<br>Dar Alta |

A figura 30 ilustra o fluxo entre os vários processos, desde a chegada do “Doente/Utente/Cliente” até abandonar o circuito, seja por Alta Médica seja porque foi

encaminhado para “Ambulatório”, “Medicina Física de Reabilitação” ou “Consulta de Acompanhamento”.

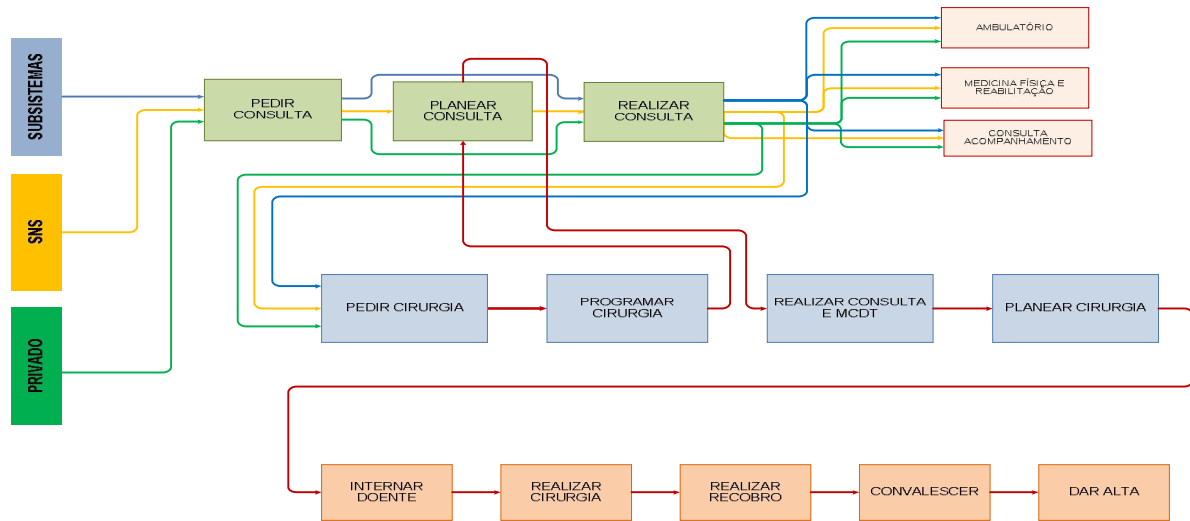


Figura 30 - Processos de Negócio do HP

O *Service System Architecture* (SSA) define, para as diferentes tarefas dentro da experiência de serviço, quais os canais e processos de apoio que são responsáveis por toda a oferta de serviço (Patrício et al.). A partir dos diversos levantamentos efectuados foi elaborada esta arquitectura que retrata a estrutura do sistema de serviços, proporcionando uma visão integrada dos recursos envolvidos na prestação de serviço (Figura 31 e Anexo E) e que é um contributo fundamental a análise de impacto no negócio, bem assim para uma melhor percepção dos diversos sistemas envolvidos. A partir desta perspectiva percebe-se a total dependência dos processos de negócio das TIC.

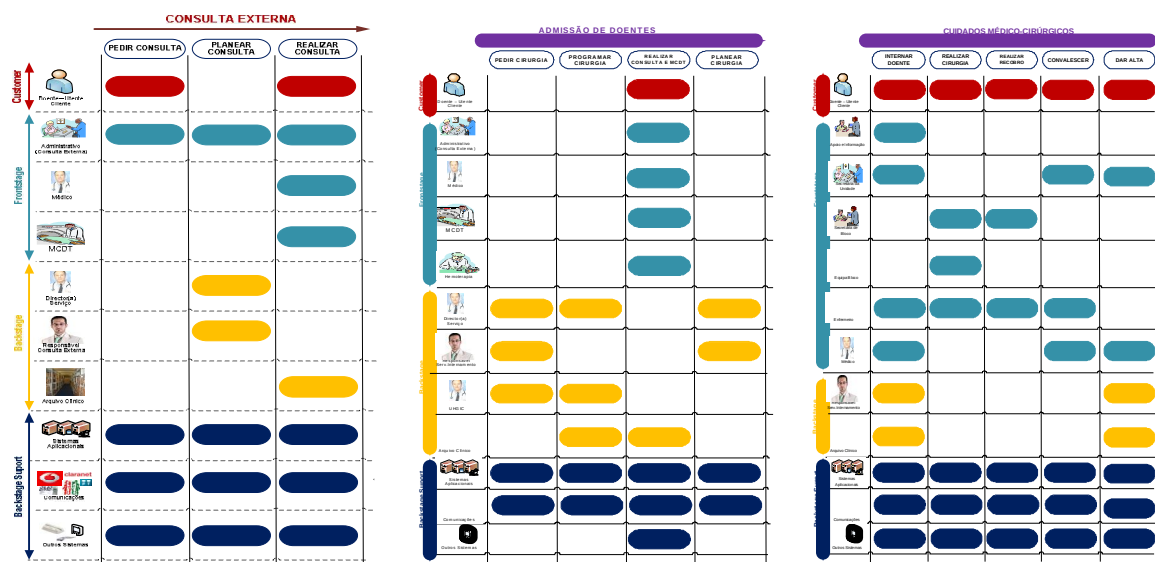


Figura 31 – Arquitectura do Sistema de Prestação de Serviço

A descoberta das relações de interdependência entre os Processos, Participantes e Plataforma, foi estabelecida através da matriz de interdependências (Figura 32) que conjuntamente com a

matriz de criticidade entre as Aplicações e as TIC permitirá estabelecer o impacto e o grau de interdependência entre os processos e os recursos que os suportam.

Identificação da Interdependência entre Processos, Participantes e Plataforma

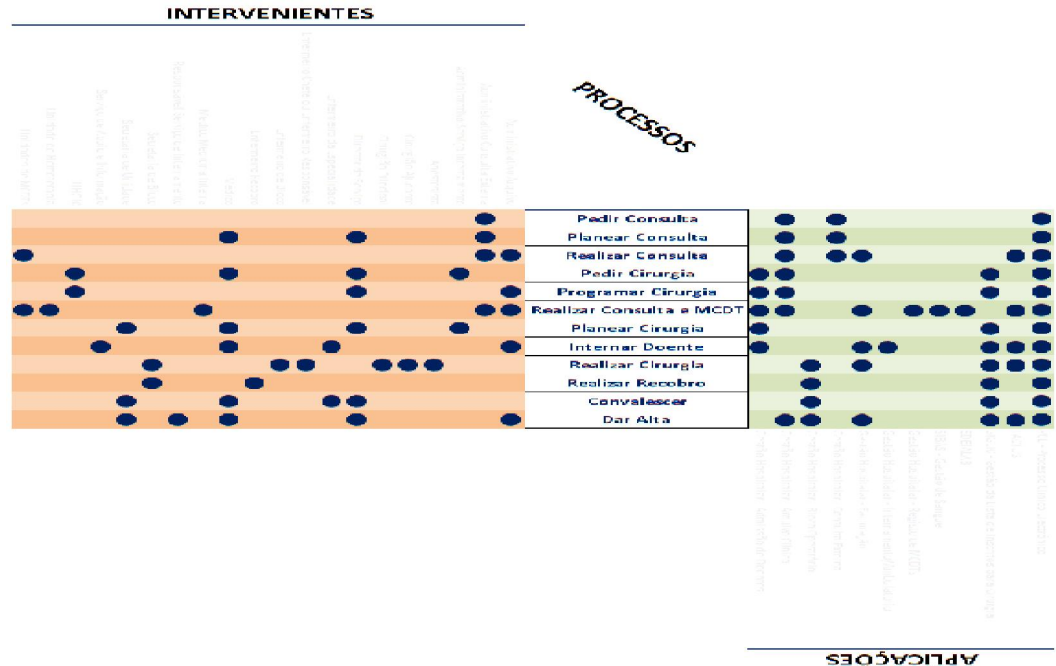


Figura 32 – Matriz de Interdependências entre Processos, Participantes e Plataforma

Identificação da Criticidade entre as Aplicações e os Sistemas Tecnológicos

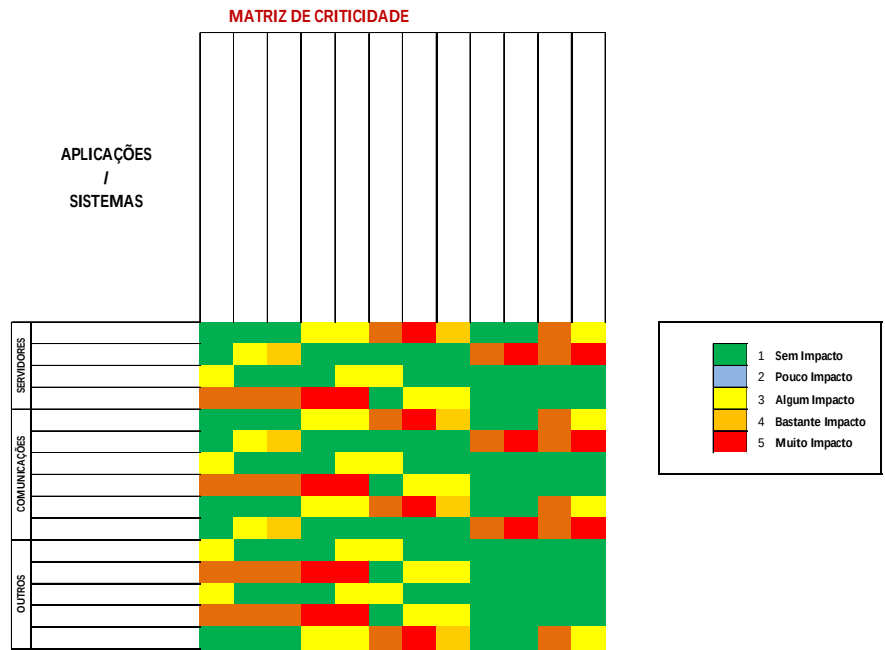


Figura 33 - Matriz de Criticidade das Aplicações / Sistemas

Na recolha da informação supra foram distribuídos os formulários (Anexos F, G e H) pelas diversas áreas de negócio, a partir dos quais foram efectuadas as análises que deram origem ao Relatório da Análise de Impacto no Negócio, com a seguinte estrutura:

### **Análise de Impacto no Negócio**

1. Introdução
  - a. Objectivos
  - b. Âmbito
  - c. Metodologia
  - d. Organização do documento
2. Área de Negócio “X”
  - a. Processos de Negócio
  - b. Actividades Críticas
  - c. Requisitos especiais
  - d. Planos de Contingência
  - e. Impacto Operacional
  - f. Resultados
3. Sumário Executivo
  - a. Relato do Impacto Financeiro Agregado
  - b. Relato do Impacto Financeiro Detalhado
  - c. Sumário do Impacto Operacional
  - d. Recursos Humanos Necessários
  - e. Prioridades de Recuperação
  - f. Processamento de Trabalho em Atraso
4. Conclusões

#### **5.4.4 Avaliação do Risco**

A temática do risco está bem presente na dialéctica e nas preocupações da rotina hospitalar. A gestão do risco é uma das competências a que o HP concede bastante atenção, nomeadamente na preparação e validação do seu Plano de Emergência.

O processo de avaliação do risco é, em regra, sustentado por um conjunto de questionários onde são elencados os diversos eventos a que a organização está sujeita e é feita uma análise com base no cenário inerente ao evento, a probabilidade de ocorrência e as consequências da sua ocorrência. No entanto, no desenvolvimento da metodologia sugerimos uma abordagem diferente, mais integradora das diversas perspectivas profissionais, utilizando instrumentos associados ao processo criativo e que conduziria ao preenchimento da referida matriz de análise do risco (Anexo J).

O processo criativo é um “processo auto-comunicacional, ou seja, como um processo no qual, a partir do repositório sempre em aberto de relações existentes, se propõem novas relações, capazes, por sua vez, de serem conjecturalmente traduzidas em novos significados.” (Carraça and Carrilho 1995). Através de técnicas de criatividade a participação de todos os intervenientes na identificação do problema ou no desenvolvimento da solução torna-se mais

fluida e geradora de sinergias colaborativas que a abordagem tradicional, que não contempla ou, pelo menos, não promove de forma evidente.

Integrado na *workshop* referida, efectuaram-se algumas actividades de *Team Work* com o objectivo de:

1. Identificar, hierarquizar e avaliar as ameaças inerentes à actividade hospitalar;

O desiderato deste objectivo foi delineado em três fases:

Fase 1 - Identificar as ameaças: Cada participante catalogou as ameaças que conseguia identificar com base na sua experiência pessoal em três classes: Ameaças Naturais, Técnicas e Humanas. Desta actividade recolheu-se as ameaças constantes na Tabela 32.

Tabela 32 - Tabela de Ameaças

| <u><b>Naturais</b></u>                                                                                                                                                                         | <u><b>Técnicas</b></u>                                                                                                                                                                                                                                                                                              | <u><b>Humanas</b></u>                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Tempestades</li><li>• Terramotos</li><li>• Incêndios / Explosões</li><li>• Ondas de calor</li><li>• Contaminação Tóxica</li><li>• Inundações</li></ul> | <ul style="list-style-type: none"><li>• Infecções Hospitalares</li><li>• Sistema Informático</li><li>• Energia, Água, Comunicações</li><li>• Avaria Equipamentos</li><li>• Perda Creditação</li><li>• Perda do Cliente</li><li>• Concorrência de Novos Hospitais</li><li>• Incêndios</li><li>• Inundações</li></ul> | <ul style="list-style-type: none"><li>• Greve</li><li>• Epidemia</li><li>• Sequestro</li><li>• Erro Humano</li><li>• Sabotagem</li><li>• Mau atendimento</li><li>• Falta de Pessoal Especializado</li><li>• Incêndios</li><li>• Inundações</li></ul> |

Fase 2 - Hierarquizar as ameaças: Cada participante pôde votar em três actividades de cada classe, que considerasse com mais impacto na actividade do HP. Este processo foi repetido até se encontrar as três ameaças por classe com maior impacto e que resultou na Tabela 33.

Tabela 33 - Tabela de Ameaças mais prováveis

| <u><b>Naturais</b></u>                                                                                                     | <u><b>Técnicas</b></u>                                                                                                            | <u><b>Humanas</b></u>                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Terramotos</li><li>• Incêndios / Explosões</li><li>• Contaminação Tóxica</li></ul> | <ul style="list-style-type: none"><li>• Infecções Hospitalares</li><li>• Sistema Informático</li><li>• Perda do Cliente</li></ul> | <ul style="list-style-type: none"><li>• Erro Humano</li><li>• Mau atendimento</li><li>• Falta de Pessoal Especializado</li></ul> |

Fase 3 - Definir os cenários, determinar a probabilidade e avaliar as consequências: Nesta fase, utilizando a técnica do Mapa Mental, solicitou-se aos participantes da *workshop* que, para cada ameaça seleccionada, respondessem às seguintes questões:

1. O que pode acontecer na ocorrência daquela ameaça? è **CENÁRIO**
2. Qual a probabilidade de isso acontecer? è **PROBABILIDADE**
3. Se acontecer, quais as consequências? è **IMPACTO**

Devido à escassez de tempo disponibilizado para esta *workshop*, a fase 3 não foi concluída integralmente, ficando, no entanto, demonstrado para algumas ameaças (Tabela 34) o

processo metodológico que levaria à construção da matriz de análise das vulnerabilidades (Anexo J)

Tabela 34 - Cenário, Probabilidade e Impacto das Ameaças

| AMEAÇA                         | CENÁRIO                      |                                                                   | PROBABILIDADE    |           | IMPACTO                        |
|--------------------------------|------------------------------|-------------------------------------------------------------------|------------------|-----------|--------------------------------|
| Terramotos                     | Interno                      | Inactividade: Infra-estruturas (Água, Energia, Comunicações, ...) | 20% a 30%        |           | Paragem Sectorial              |
|                                | Externo                      | Inacessibilidade                                                  | Grau Elevado     | 75% a 80% | Paragem do Hospital            |
| Incêndios / Explosões          | Impacto Sectorial Temporário |                                                                   | Grande Incêndio  | 20%       | Paragem do Hospital            |
|                                |                              |                                                                   | Pequeno Incêndio | 80%       | Paragem Sectorial              |
| Contaminação Tóxica            |                              |                                                                   |                  |           |                                |
| Infecções Hospitalares         |                              |                                                                   |                  |           |                                |
| Sistema Informático            | Organização                  | Lentidão                                                          | 40%              |           | Imagem<br>Qualidade do Serviço |
|                                |                              | Erro                                                              | 10% a 20%        |           |                                |
|                                |                              | Inacessibilidade                                                  | Temporária       | 20%       | Paragem Operações Internas     |
|                                | Exportação de Dados          |                                                                   | Longo Prazo      | 1%        |                                |
| Perda do Cliente               |                              |                                                                   |                  |           |                                |
|                                |                              |                                                                   |                  |           |                                |
| Erro Humano                    |                              |                                                                   |                  |           |                                |
| Mau Atendimento                |                              |                                                                   |                  |           |                                |
| Falta de Pessoal Especializado |                              |                                                                   |                  |           |                                |

A reduzida janela de oportunidade para desenvolver esta metodologia no HP não permitiu prosseguir as actividades que conduziram à validação integral da metodologia. As duas fases restantes serão descritas conceptualmente.

#### 5.4.5 Elaboração do BCP

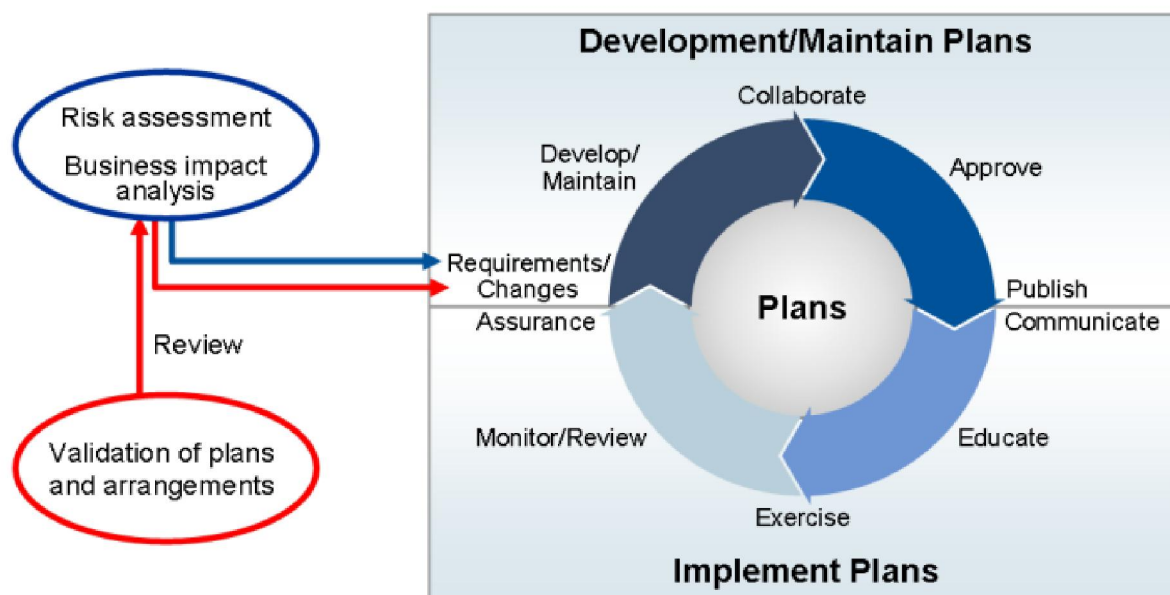
O BCP deve descrever os procedimentos de escalada de incidentes que permitam que o incidente tenha a definição de desastre. Se um incidente é, ou pode ser, um desastre, a decisão a tomar pode ser a de activar uma equipa de intervenção ou activar o plano (Beatty 2007).

O BCP deve seguir um processo formal standard, não de forma *ad-hoc*, que enderece os riscos de disponibilidade e as necessidades do negócio (Witty and Stevens 2010):

- Instituinto quais os riscos de disponibilidade e necessidades do negócio, incluindo os requisitos de conformidade e os pontos de fragilidade;
- Atendendo ao tipo de destinatários. Um BCP destinado aos utilizadores finais utiliza uma linguagem diferente do que tem por destinatários os administradores das TIC;
- Instituinto um processo que garanta consenso entre as áreas de negócio, TI e outros *stakeholders* do conteúdo do BCP;
- Definindo um standard e uma estrutura para o documento e procedimentos e orientações standards;
- Obtendo e compreendendo um cultura transfuncional;

- Definindo o repositório do *BCP*;

A estratégia no desenvolvimento do *BCP* parte das actividades desenvolvidas para obtenção da *BIA*, para determinar o impacto e os recursos de recuperação necessários aquando de uma disrupção, e da Avaliação do Risco, para identificar a causa da disrupção. Como se verificou, ambas actividades requerem os *inputs* dos gestores dos processos de negócio e dos administradores dos diversos sistemas de suporte, das TIC às instalações.



Fonte: Gartner Research (Witty and Stevens 2010)

Figura 34 - Estratégia no desenvolvimento de um *BCP*

O *BCP* é um plano de acção pelo que deve ser sucinto e objectivo, devendo incluir a seguinte informação:

- Título, Controlo do Documento, Data e Versão, Registo de Confidencialidade;
- Índice;
- Pressupostos e Limitações do plano;
- Alertas, invocações, notificações e instruções de acção;
- Lista dos contactos internos e externos, incluindo os membros do Comité de Continuidade;
- Informações sobre a reafecção dos colaboradores, localização de *standby* e como obter acesso;
- Plano de acções prioritárias e cronograma das acções a iniciar e completar;
- Lista dos materiais vitais e instruções de como obtê-los;
- Requisitos dos equipamentos e recursos necessários para a recuperação, prazo em que devem ser disponibilizados e como obtê-los;
- Requisitos de comunicação, reporte e *logging*;
- Instruções de gestão da comunicação com os *média*;
- Detalhe minucioso dos procedimentos de suporte técnico, operacional e administrativo, planos, desenhos, esquemas, plantas, etc., e referências de como obtê-los;

O *BCP* não deve incluir detalhes da *BIA*, Avaliação do Risco, Testes e Relatórios de Auditoria efectuados, Metodologia e Instruções de Manutenção e outra informação que não seja necessária para as acções de recuperação.

#### **5.4.6 Monitorização do Risco e Teste**

Um *BCP* nunca está completo. Quantos mais detalhados forem os procedimentos de acompanhamento, mais efectivo será o plano. O normal é que um plano vá sendo melhorado, decorrendo das actividades de Teste e Monitorização, devendo incluir um planeamento calendarizado dessas actividades de Auditoria e Revisão. Um dos objectivos da auditoria e revisão do *BCP* é encontrar áreas de melhoria que possam ser incluídas nos planos de revisão. Outras das razões tem a ver com a necessidade de o *BCP* se manter actualizado, havendo um rigoroso controlo e gestão das alterações e do seu impacto nos procedimentos de recuperação.



## 6 Conclusões

*“O Hospital de Elvas vai passar o fim-de-semana sem climatização. Um dos dois geradores do sistema de refrigeração do Hospital Santa Luzia avariou-se durante a madrugada e só poderá ser reparado na segunda-feira por falta de peças. O sistema de climatização é fornecido por dois geradores, um ficou avariado. A empresa que faz a manutenção já identificou o problema vai segunda-feira de manhã, por falta de peças, imediatamente resolver”* – Rádio Renascença, 2-07-2010 – 21:32 (RR 2010)

Para ilustrar a necessidade de uma política de continuidade recorre-se com frequências às calamidades ou desastres de grande dimensão que, em regra, ocorrem noutros países. A notícia retrata a situação em que se encontram muitos hospitais e a evidência do impacto de um incidente localizado pode ter no funcionamento de um hospital.

Esta situação ilustra diversas lacunas:

- Ausência de mecanismos de contingência para minimizar o impacto da avaria;
- Falta de redundância de sistemas críticos no funcionamento de um hospital inserido numa região cujas temperaturas médias nesta época são superiores a 30°;
- Incapacidade da empresa de manutenção em resolver ou minimizar o efeito da avaria durante três dias. Provavelmente a peça terá de ser importada por não existir um stock mínimo de substituição.

Esta situação é possível multiplicar-se tantas vezes quantas as ocorrências. A investigação efectuada demonstrou um quadro de quase ausência de uma política de gestão continuidade nos hospitais portugueses:

- 83% não dispõe de um Plano de Continuidade do Negócio;
- 78% não dispõe de um Plano de Recuperação de Desastre
- 15% não dispõe de um Plano de Emergência.

Co-relacionando com o Nível de Maturidade dos Sistemas de Informação e considerando os hospitais “HIS/CIS Avançado” ou superior:

- 75% não dispõe de um Plano de Continuidade do Negócio;
- 67% não dispõe de um Plano de Recuperação de Desastres;
- 8% não dispõe de um Plano de Emergência.

Este estudo demonstrou a lacuna existente nesta área e, ao mesmo tempo, a oportunidade de desenvolvimento, pois 90% dos questionados consideram esta política “Muito Importante” ou “Importante”, justificando com “Outras Prioridades” o adiamento da sua implementação.

Investigação paralela demonstrou a ausência desta temática em Portugal, quer na investigação científica, com excepção da componente associada à segurança da informação, quer da oferta de formação. Uma pesquisa aos currículos dos diversos cursos superiores não obteve qualquer resultado, tendo encontrado a oferta de um curso de formação ministrado por um Centro de Formação Profissional.

Evidência deste contexto é a ausência de regulamentação que contribua para priorizar o desenvolvimento desta política nas organizações e baixa exigência dos *stakeholders* dos sistemas de saúde de processos de auditoria que avaliem a conformidade dos hospitais com as boas práticas internacionais.

O caso de estudo desenvolvido no Hospital, pese embora as limitações temporais que condicionaram o âmbito e a extensão do projecto, permitiram criar os alicerces de uma política de gestão de continuidade do negócio. A análise de impacto no negócio, conjugada com a Avaliação do Risco possibilita a definição de uma estratégia com vista a minimizar as lacunas existentes na infra-estrutura de suporte ao negócio e ao desenvolvimento de um plano de continuidade.

Na opção metodológica pelo processo de desenvolvimento há elementos comuns aos vários standards internacionais que importa destacar, sem prejuízo de cada hospital optar pela orientação de conformidade que melhor se adaptar ao seu contexto socioeconómico. Destacamos:

- O patrocínio e envolvimento da administração de topo neste processo;
- Um extenso e pormenorizado levantamento dos processos de negócio, dos recursos envolvidos e das relações de interdependência, que permita conhecer as capacidades e limitações dos sistemas críticos associados à missão da organização;
- Quantificação e qualificação do impacto no negócio das quebras de serviço;
- Avaliação dos cenários, probabilidades e consequências dos riscos emergentes, que permita uma profunda análise de vulnerabilidades;
- Desenvolvimento de planos de mitigação e projectos que aumentem a resiliência da organização;
- Desenvolvimento, para cada área de negócio hospitalar, de planos de contingência, tendo em atenção a criticidade de cada departamento no conjunto de actividade do hospital;
- Desenvolvimento de uma política de comunicação que envolva todas as equipas, internas e externas, de recuperação;
- Aplicação de um programa regular de sensibilização, formação, teste, auditoria, manutenção e revisão dos planos de continuidade de cada área hospitalar e do plano global;

A sustentabilidade e *survivability* das organizações em geral e dos hospitais em particular constrói-se com um processo continuado de mitigação dos riscos que incorpore a cultura organizacional e que envolva todos os intervenientes no desenvolvimento de um plano de continuidade. Como referimos no início deste trabalho, **não chovia quando Noé começou a construir a arca!**

Porto, 20 de Julho de 2010

Manuel Vítor de Lima Vieira Alves

---

## Referências e Bibliografia

- Alves, Vitor V. *Inquérito sobre a Gestão da Continuidade nos hospitais portugueses* 2010. Available from <https://spreadsheets.google.com/viewform?hl=en&formkey=dDB0b09URzdOaWZJSXdPQnlhVWpFc3c6MQ#gid=0>.
- The American Heritage Dictionary of the English Language*. 2006. Boston: Houghton Mifflin.
- Beatty, Gregg C. 2007. Emergency response and operations. In *The definitive handbook of business continuity management*, edited by A. Hiles. Chichester, England ; Hoboken, NJ, : John Wiley & Sons.
- Bierenbaum, A. B., B. Neiley, and C. R. Savageau. 2009. Importance of business continuity in health care. *Disaster Medicine and Public Health Preparedness* 3 (2):7-9.
- Bilhim, João Abreu de Faria. 2004. *Teoria organizacional estruturas e pessoas*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Brand, Koen, and Harry Boonen. 2004. *IT governance based on CobiT : a pocket guide, Best practice IT management*. Zaltbommel: Van Haren Publishing.
- BS25999-2. British Standard 25999 - Part 2: Specification. In *British Standard*. London: British Standards Institution.
- BSI. *British Standards Institute* [cited 29-06-2010. Available from [www.bsigroup.com](http://www.bsigroup.com).
- Caralli, Richard A. , Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young. 2010. *Cert Resilience Management Model, Version 1.0*. edited by S. E. Institute: Carnegie Mellon University.
- Carraça, João, and Manuel Maria Carrilho. 1995. *Partilha e Conhecimento*. Lisboa: Fundação Calouste Gulbenkian.
- Cornish, Malcolm. 2007. The Business Continuity Planning Methodology. In *The definitive handbook of business continuity management*, edited by A. Hiles. Chichester, England ; Hoboken, NJ: John Wiley & Sons.
- Domage, Eric. 2010. *What Is The Future of Data (Security & Storage)? Key trends & Observations*. C.C.Belém, Lisboa.
- DRII. *Disaster Recovery Institute International* [cited 29-06-2010. Available from [www.drii.org](http://www.drii.org).
- Drucker, Peter Ferdinand. 1998. The coming of the new organization. *Harvard business review on knowledge management*:1-19.
- Erlich, Leonardo. 2004. *Plano de Continuidade de Negócios: Uma pesquisa exploratória na perspectiva estratégica no âmbito da segurança da informação*. MsC, Departamento de Administração da Pontifícia Universidade Católica do Rio de Janeiro.
- Gibb, Forbes, and Steven Buchanan. 2006. A framework for business continuity management. *International Journal of Information Management* 26 (2):128-141.
- Ginzberg, Eli. *Tomorrow's hospital a look to the twenty-first century*. Yale University Press 1996. Available from <http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=53003>.
- Heath, Robert. 2007. A crisis management perspective of business continuity. In *The definitive handbook of business continuity management*. Chichester, England John Wiley & Sons: xxx.

- Herbane, Brahim, Dominic Elliott, and Ethné M. Swartz. 2004. Business Continuity Management: time for a strategic role? *Long Range Planning* 37 (5):435-457.
- Hiles, Andrew. 2007. International perspectives, standards and sources. In *The definitive handbook of business continuity management*. Chichester, England John Wiley & Sons: xxx.
- . 2007. Introduction. In *The definitive handbook of business continuity management*. Chichester, England John Wiley & Sons: xxx.
- HSNW. *Gartner: only 6 percent of companies survive longer than two years after losing data 2010* [cited 31-05-2010. Available from <http://homelandsecuritynewswire.com/gartner-only-6-percent-companies-survive-longer-two-years-after-losing-data>.
- IDC. *Healthcare IT Maturity Model 2008* [cited 15-03-2010. Available from <http://www.idc-hi.com/getdoc.jsp?containerId=HI210231>.
- . 2009. Impacto da Crise Financeira – Mercado das TIC – Portugal vs Europa: Análise e Previsões 2008-2012. IDC.
- ITGI. *COBIT4. 1* 2007 [cited 29-06-2010. Available from <http://www.isaca.org>.
- ITIL. *IT Infrastructure Library* [cited 29-06-2010. Available from [www.ital-officialsite.com](http://www.ital-officialsite.com).
- Jordan, Ernest. 2005. IT Service Continuity Assessment. *SSRN eLibrary*.
- Kaplan, Stan. 1997. The Words of Risk Analysis. *Risk analysis : an official publication of the Society for Risk Analysis*. 17 (4):407.
- Katsikas, Sokratis K. 2000. Health care management and information systems security: awareness, training or education? *International Journal of Medical Informatics* 60 (2):129-135.
- Khorasani, Ramin. 2008. Business Continuity and Disaster Recovery: PACS as a Case Example. *Journal of the American College of Radiology* 5 (2):144-145.
- Lapão, L. Velez. 2007. Survey on the Status of the Hospital Information Systems in Portugal. *Methods of information in medicine. Methodik der Information in der Medizin*. 46 (4):493.
- Laudon, Kenneth C., and Jane Price Laudon. 2009. *Essentials of management information systems managing the digital firm*. Upper Saddle River, N.J: Pearson Prentice-Hall.
- Marczyk, Geoffrey R., David DeMatteo, and David Festinger. 2005. *Essentials of research design and methodology, Essentials of behavioral science series*. Hoboken, N.J.: John Wiley & Sons.
- Mendonca, D., G. E. G. Beroggi, D. van Gent, and W. A. Wallace. 2006. Designing gaming simulations for the assessment of group decision support systems in emergency response. *Safety Science* 44 (6):523-535.
- Noakes-Fry, Kristen, and Trude Diamond. 2001. Business Continuity and Disaster Recovery Planning and Management: Perspective. edited by G. Research: Gartner Research.
- Normann, R., and R. Ramírez. 1993. From value chain to value constellation: designing interactive strategy. *Harvard business review* 71 (4).
- O'Hehir, Mike. 2007. What is a business continuity planning strategy? In *The definitive handbook of business continuity management*, edited by A. Hiles. Chichester, England ; Hoboken, NJ, : John Wiley & Sons.
- Patrício, Lia, Raymond P. Fisk, João Falcão Cunha, and Larry Constantine. Service System Design for Value Co-Creation: From Value Constellation to Service Experience Blueprinting
- Pitt, Michael, and Sonia Goyal. 2004. Business continuity planning as a facilities management tool. *Facilities* 22 (3-4):87-99.

- Post, J. E., L. E. Preston, and S. Sachs. 2002. Managing the Extended Enterprise: The New Stakeholder View. *California Management Review* 45:6-28.
- Quirchmayr, Gerald. 2004. Survivability and business continuity management. In *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32*. Dunedin, New Zealand: Australian Computer Society, Inc.
- Raja, K. Iyer, and Bandyopadhyay Kakoli. 2000. Managing technology risks in the healthcare sector: disaster recovery and business continuity planning. *Disaster Prevention and Management* 9 (4):257-270.
- RR. *Hospital de Elvas sem climatização* 2010 [cited 02-07-2010. Available from [http://www.rr.pt/informacao\\_detalhe.aspx?fid=92&did=110910](http://www.rr.pt/informacao_detalhe.aspx?fid=92&did=110910).
- Sampieri, Roberto Hernández, Carlos Fernández Collado, and Pilar Baptista Lucio. 2006. *Metodologia de pesquisa*. São Paulo: McGraw-Hill.
- Santos, António Carvalho. 2007. Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação Escola de Engenharia, Universidade do Minho, Braga.
- Saúde, Ministério da. *Portal da Saúde* 2010. Available from <http://www.min-saude.pt/>.
- SCMP. 2010. *Hospital da Prelada* 2010 [cited 27-05-2010 2010]. Available from <http://www.scmp.pt>.
- Serrano, António, and Nuno Jardim. 2007. *Disaster Recovery: um paradigma na Gestão da Continuidade*. Lisboa: FCA - Editora de Informática, Lda.
- Shortliffe, Edward Hance, and James J. Cimino. 2006. *Biomedical informatics : computer applications in health care and biomedicine*. New York, NY: Springer.
- Smith, David. 2003. Business Continuity and Crisis Management. *Management Quarterly* January 2003.
- Snedaker, Susan. 2007. *Business continuity & disaster recovery for IT professionals*. Burlington, MA: Syngress.
- Stanton, R. 2005. Beyond disaster recovery: the benefits of business continuity. *Computer Fraud and Security* 2005 (7):18-19.
- Sterbenz, James P. G., David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* 54 (8):1245-1265.
- Vancoppenolle, Geert. 2007. What are we planning for? In *The definitive handbook of business continuity management*, edited by A. Hiles. Chichester, England ; Hoboken, NJ: John Wiley & Sons.
- Vose, David. 2000. *Risk analysis : a quantitative guide*. Chichester; New York: Wiley.
- Witty, Roberta J. , and Les Stevens. 2010. Ten Best Practices for Creating and Maintaining Effective Business Continuity Management Plans. *Gartner Research* (G00174201).
- Zambon, Emmanuele, Damiano Bolzoni, Sandro Etalle, and Marco Salvato. 2007. A Model Supporting Business Continuity Auditing & Planning in Information Systems. In *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*. Silicon Valley, USA.
- Zhu, Weichun, Irene K. H. Chew, and William D. Spangler. 2005. CEO transformational leadership and organizational outcomes: The mediating role of human-capital-enhancing human resource management. *The Leadership Quarterly* 16 (1):39-52.

**Anexo A – Inquérito sobre a Gestão de Continuidade do Negócio nos hospitais portugueses – carta de apresentação**

Exmo. Senhor

**Presidente do Conselho de Administração do**

Porto, 12-04-2010

**Assunto: Inquérito sobre a Gestão de Continuidade do Negócio nos hospitais portugueses**

Exmo. Senhor,

No contexto actual da sociedade, a emergência de factores disruptivos que colocam em causa a continuidade da prestação do serviço das organizações, é um elemento central da agenda da gestão. No caso das organizações prestadoras de cuidados de saúde, como os hospitais, este factor reveste-se de particular relevância.

Na senda de perceber o “Estado da Arte” desta temática no Hospital que V. Ex.<sup>a</sup> administra e enquadrado numa investigação conducente à Dissertação de Mestrado em Engenharia de Serviços e Gestão da Faculdade de Engenharia da Universidade do Porto, sobre o tema da “Gestão da Continuidade dos Negócios em contexto hospitalar”, solicitamos de V. Ex.<sup>a</sup> a indispensável colaboração na resposta ao questionário que anexamos.

O questionário é confidencial e os dados serão unicamente utilizados neste trabalho de investigação. Aproveitamos o ensejo para prestar todos os esclarecimentos e informações, bem assim como facultar o acesso ao relatório final da investigação.

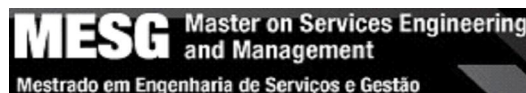
Agradecendo a colaboração de V. Ex.<sup>a</sup> e do hospital que administra, subscrevemo-nos

Com os melhores cumprimentos,

Manuel Vítor de Lima Vieira Alves (Dr.)

António Carvalho Brito (Prof. Doutor)  
(Professor Orientador)

## Anexo B – Inquérito sobre a Gestão de Continuidade do Negócio nos hospitais portugueses



### INQUÉRITO

## Gestão da Continuidade do Negócio nos Hospitais Portugueses

A Gestão da Continuidade do Negócio pode ser definida como “um processo holístico de gestão, que identifica potenciais ameaças para uma organização e os impactos para as operações do negócio que essas ameaças, se concretizadas, poderiam causar, e que fornece um quadro para a construção da resiliência organizacional, com capacidade para uma resposta eficaz e que proteja os interesses dos seus principais *stakeholders*, a reputação, a marca e as actividades criadoras de valor”<sup>1</sup>.

A Gestão da Continuidade do Negócio, enquanto estratégia que visa a Continuidade das Operações da Organização, decorre do desenvolvimento e implementação de três planos:

1. **Plano de Continuidade do Negócio**, que descreve os processos de negócio alternativos, que permitam ao hospital continuar a operar;
2. **Plano de Recuperação em Caso de Desastre** (*Disaster Recovery*), que descreve a estratégia de recuperação dos Datacenters numa localização alternativa;
3. **Plano de Emergência**, interno e externo, que descreve os procedimentos a efectuar em situação de incidente relativamente a instalações, pessoas, etc.

Com o presente questionário pretendemos obter uma visão desta temática nos hospitais portugueses, independentemente da natureza jurídica.

**MUITO OBRIGADO PELO TEMPO DISPENDIDO NO PREENCHIMENTO DESTES QUESTIONÁRIOS. POR FAVOR RESPONDA ÀS QUESTÕES ASSINALANDO COM UM 'X' A(S) RESPOSTA(S). DEVOLVA O QUESTIONÁRIO UTILIZANDO O ENVELOPE ANEXO.**

**O QUESTIONÁRIO É CONFIDENCIAL E OS SEUS DADOS DESTINAM-SE UNICAMENTE A INVESTIGAÇÃO CIENTÍFICA. SE PRETENDER OBTER UMA CÓPIA DO RELATÓRIO FINAL OU QUALQUER ESCLARECIMENTO, AGRADECEREMOS O SEU CONTACTO PARA:**

Investigador:

- Manuel Vítor de Lima Vieira Alves  
E-mail: vitor.vieira.alves@gmail.com

Professor Orientador:

- Prof. Doutor António Carvalho Brito  
FEUP – DEIG  
E-mail: acbrito@fe.up.pt

<sup>1</sup> BS 25999-1 British Standards Institution's Code of Practice for Business Continuity Management

### Classificação do hospital:

**Q1** Classifique o hospital de acordo com a natureza jurídica:

☐ Público (EPE) ☐ Público (Outro) ☐ Privado ☐ Sistema Social

**Q2** Classifique o hospital de acordo com a lotação oficial de camas:

£ <100    £ 100 – 250    £ 250 – 500    £ 500 – 1000    £ > 1000

**Q3** Classifique o hospital de acordo com as valências de serviço:

|            |                |                    |
|------------|----------------|--------------------|
| £ Cirurgia | £ Medicina     | £ Mulher e Criança |
| £ Urgência | £ Saúde Mental | £ Consulta Externa |
| £ MCDT     | £ Ambulatório  | £ Hospital de Dia  |
| £ _____    | £ _____        | £ _____            |

### Maturidade dos Sistemas de Informação / Tecnologias de Informação e Comunicação (SI/TIC):

**Q4** Assinale as aplicações suportadas pelas Tecnologias de Informação e Comunicação?

| Âmbito dos SI/TIC                                                                                                                                                                                                                     | Portfólio aplicacional / Portfólio de Soluções TI  |                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------|
| Implementação de sistemas informáticos para suportar as funções nucleares a nível administrativo e financeiro. (funções de back-office)                                                                                               | £ Registo de doentes                               | £ Salários                                       |
|                                                                                                                                                                                                                                       | £ Facturação                                       | £ Ferramentas de escritório electrónico          |
|                                                                                                                                                                                                                                       | £ Contas correntes                                 | £ LAN                                            |
|                                                                                                                                                                                                                                       | £ Contabilidade                                    |                                                  |
| Implementação de sistemas informáticos para suportar funções mais sofisticadas a nível administrativo, financeiro e hoteleiro (funções de back-office) e as funções nucleares a nível da gestão de doentes (funções de front-office). | £ Agendamento de actos médicos                     | £ Gestão de stocks                               |
|                                                                                                                                                                                                                                       | £ Registo de actos médicos                         | £ Correio electrónico                            |
|                                                                                                                                                                                                                                       | £ Gestão do arquivo clínico                        | £ Acesso à internet                              |
|                                                                                                                                                                                                                                       | £ Logística                                        | £ Intranet                                       |
| Implementação de sistemas informáticos para suportar as funções nucleares ao nível da gestão da informação clínica (base para o Processo Clínico Electrónico).                                                                        | £ LIS – Laboratory Information System              | £ Extranet – EDI                                 |
|                                                                                                                                                                                                                                       | £ RIS – Radiology Information System               | £ PACS – Picture Archiving and Computing Systems |
|                                                                                                                                                                                                                                       | £ Bloco Operatório                                 |                                                  |
| Implementação de sistemas informáticos para suportar funções mais sofisticadas ao nível da gestão da informação clínica (Processo Clínico Electrónico).                                                                               | £ Processo Clínico Electrónico                     | £ Portal colaborativo                            |
|                                                                                                                                                                                                                                       | £ Prescrição electrónica                           | £ WLAN                                           |
|                                                                                                                                                                                                                                       | £ Notas de enfermagem                              | £ Ferramentas colaborativas                      |
|                                                                                                                                                                                                                                       | £ Portal do doente                                 | £ Wireless point of care                         |
| Implementação de sistemas informáticos para gerir os repositórios de informação clínica e de negócio (Business Intelligence).                                                                                                         | £ Sistemas de informação de Gestão (Datawarehouse) | £ Videoconferência                               |
| Desenvolvimento de iniciativas na área da telemedicina, da monitorização remota de doentes e de partilha de informação clínica com outras instituições de saúde.                                                                      | £ Portais de saúde                                 | £ Segurança                                      |
|                                                                                                                                                                                                                                       | £ Sistemas de apoio à decisão clínica              | £ WAN                                            |

Fonte: IDC Health Insights (<http://www.idc-hi.com>)

## Gestão da Continuidade do Negócio

**Importância** da Gestão da Continuidade do Negócio no serviço hospitalar e a **Percepção do Risco**:

**Q5** Qual o grau de importância que atribui à existência de uma política de Gestão da Continuidade no hospital?

☐ Muito Importante      ☐ Importante      ☐ Pouco Importante      ☐ Nada Importante

**Q6** Na sua opinião esta política deve ser conduzida por: (*Escolha uma opção*)

☐ Conselho de Administração      ☐ Direcção de Gestão do Risco      ☐ Equipa Técnica Específica  
☐ Direcção de Sistemas de Informação      ☐ Direcção de Equipamentos e Instalações      ☐ Gestor Sénior  
☐ \_\_\_\_\_

**Q7** Classifique, numa escala de 1 (pouco) a 5 (muito) a importância dos seguintes riscos para o negócio hospitalar:

|                                                   |                                                 |
|---------------------------------------------------|-------------------------------------------------|
| j k l m n - Ameaças electrónicas (vírus)          | j k l m n - Incêndios                           |
| j k l m n - Doenças (ex. pandemia)                | j k l m n - Falhas na logística de fornecimento |
| j k l m n - Ameaças atmosféricas (temporais, ...) | j k l m n - Greves do pessoal                   |
| j k l m n - Ameaças à infra-estrutura             | j k l m n - Acidentes                           |
| j k l m n - Inundações                            | j k l m n - Assaltos                            |

**Quebras de Serviço** ou Sistemas Interrompidos:

**Q8** No ano de 2009 foram registadas quebras de serviço motivadas por **falhas não programadas** dos sistemas?

☐ Sim é Questão **Q9**

☐ Não é Questão **Q13**

**Q9** Em termos anuais, qual a duração das quebras em n.º de dias?

☐ <1      ☐ [1-2]      ☐ [3-5]      ☐ > 5      ☐ Não determinado

**Q10** Foi determinado o impacto no negócio dessas quebras? Qual o valor estimado?

☐ Sim, € \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_,00      ☐ Não

**Q11** Assinale as principais causas pela quebra do serviço e o n.º de ocorrências:

|                                                      |                                                         |                                                        |
|------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------|
| <input type="checkbox"/> Falhas dos Sistemas de TI 5 | <input type="checkbox"/> Falha nas comunicações 5       | <input type="checkbox"/> Falta de competências chave 5 |
| <input type="checkbox"/> Condições atmosféricas 5    | <input type="checkbox"/> Falta de água, luz, gás, ... 5 | <input type="checkbox"/> Incêndio 5                    |
| <input type="checkbox"/> Falha de pessoas 5          | <input type="checkbox"/> Doença de colaboradores        | <input type="checkbox"/> Falha no abastecimento 5      |

**Q12** Das causas identificadas, quais estão cobertas pela política Gestão da Continuidade do Negócio?

|                                                    |                                                       |                                                      |
|----------------------------------------------------|-------------------------------------------------------|------------------------------------------------------|
| <input type="checkbox"/> Falhas dos Sistemas de TI | <input type="checkbox"/> Falha nas comunicações       | <input type="checkbox"/> Falta de competências chave |
| <input type="checkbox"/> Condições atmosféricas    | <input type="checkbox"/> Falta de água, luz, gás, ... | <input type="checkbox"/> Incêndio                    |
| <input type="checkbox"/> Falha de pessoas          | <input type="checkbox"/> Doença de colaboradores      | <input type="checkbox"/> Falha no abastecimento      |

### Plano de Continuidade do Negócio:

**Q13** O Hospital dispõe de Plano de Continuidade de Negócio?

☐ Sim é Questão **Q14**

☐ Não é Questão **Q22**

**Q14** Quantas pessoas estão envolvidas na manutenção do Plano de Continuidade de Negócio?

☐ [1-2]      ☐ [3-5]      ☐ [5-10]      ☐ > 10

**Q15** Utiliza algum software para planeamento e manutenção do Plano de Continuidade de Negócio?

☐ Sim: \_\_\_\_\_      ☐ Não

**Q16** O Plano de Continuidade de Negócio foi desenvolvido por:

☐ Equipa técnica do hospital      ☐ Empresa de *outsourcing*

**Q17** Efectua testes com que periodicidade?

---

|                                  |                                |                               |                                                     |
|----------------------------------|--------------------------------|-------------------------------|-----------------------------------------------------|
| <input type="checkbox"/> 6 Meses | <input type="checkbox"/> Anual | <input type="checkbox"/> Bial | <input type="checkbox"/> Sem periodicidade definida |
|----------------------------------|--------------------------------|-------------------------------|-----------------------------------------------------|

**Q18** O Plano de Continuidade de Negócio inclui formação e sensibilização dos colaboradores?

|                              |                              |
|------------------------------|------------------------------|
| <input type="checkbox"/> Sim | <input type="checkbox"/> Não |
|------------------------------|------------------------------|

**Q18** O PNC inclui formação e sensibilização dos colaboradores?

|                              |                              |
|------------------------------|------------------------------|
| <input type="checkbox"/> Sim | <input type="checkbox"/> Não |
|------------------------------|------------------------------|

**Q19** Qual a periodicidade na preparação e manutenção do PNC?

|                                 |                                   |                                     |                                    |                                |                                  |
|---------------------------------|-----------------------------------|-------------------------------------|------------------------------------|--------------------------------|----------------------------------|
| <input type="checkbox"/> Mensal | <input type="checkbox"/> Bimensal | <input type="checkbox"/> Trimestral | <input type="checkbox"/> Semestral | <input type="checkbox"/> Anual | <input type="checkbox"/> Nenhuma |
|---------------------------------|-----------------------------------|-------------------------------------|------------------------------------|--------------------------------|----------------------------------|

**Q20** Indique o nº de dias/ano despendidos na preparação e manutenção do PNC

\_\_\_\_\_ dias/ano

**Q21** Quem assume a responsabilidade pelo PCN?

|                                              |                                             |                                                          |
|----------------------------------------------|---------------------------------------------|----------------------------------------------------------|
| <input type="checkbox"/> Gestor sénior       | <input type="checkbox"/> Equipa do PNC      | <input type="checkbox"/> Departamento de Gestão de Risco |
| <input type="checkbox"/> Administração       | <input type="checkbox"/> Equipa Operacional | <input type="checkbox"/> _____                           |
| <input type="checkbox"/> Direcção dos SI/TIC |                                             |                                                          |

è Questão **Q24**

**Q22** Prevê desenvolver um PCN no ano:

|                                                                                               |                                       |                                                   |
|-----------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------|
| <input type="checkbox"/> 2010 - <input type="checkbox"/> 2011 - <input type="checkbox"/> 2012 | <input type="checkbox"/> Não definido | <input type="checkbox"/> Não tenciona implementar |
|-----------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------|

**Q23** Quais os motivos que ditaram o adiamento desta decisão? (Assinale e indique o grau de importância)

|                                                                         |                                                             |
|-------------------------------------------------------------------------|-------------------------------------------------------------|
| <input type="checkbox"/> Montante Investimento. 5 <sup>a</sup>          | <input type="checkbox"/> Outras prioridades. 5 <sup>a</sup> |
| <input type="checkbox"/> Recursos Técnicos qualificados. 5 <sup>a</sup> | <input type="checkbox"/> _____. 5 <sup>a</sup>              |

**Q24** Qual o grau de importância que atribui à existência de um PCN?

|                                           |                                     |                                           |                                          |
|-------------------------------------------|-------------------------------------|-------------------------------------------|------------------------------------------|
| <input type="checkbox"/> Muito Importante | <input type="checkbox"/> Importante | <input type="checkbox"/> Pouco Importante | <input type="checkbox"/> Nada Importante |
|-------------------------------------------|-------------------------------------|-------------------------------------------|------------------------------------------|

**Q25** O hospital dispõe de uma **Análise do Impacto do Negócio (AIN)**?

|                              |                                                   |
|------------------------------|---------------------------------------------------|
| <input type="checkbox"/> Sim | <input type="checkbox"/> Não è Questão <b>Q30</b> |
|------------------------------|---------------------------------------------------|

**Q26** A Análise de Impacto no Negócio cobre todos os Departamentos e Processos?

|                              |                              |
|------------------------------|------------------------------|
| <input type="checkbox"/> Sim | <input type="checkbox"/> Não |
|------------------------------|------------------------------|

**Q27** A informação recolhida pela AIN é utilizada somente pela equipa de Gestão de Continuidade?

|                              |                              |
|------------------------------|------------------------------|
| <input type="checkbox"/> Sim | <input type="checkbox"/> Não |
|------------------------------|------------------------------|

**Q28** Com que frequência efectuam uma AIN?

|                                |                               |                                     |                                                  |
|--------------------------------|-------------------------------|-------------------------------------|--------------------------------------------------|
| <input type="checkbox"/> Anual | <input type="checkbox"/> Bial | <input type="checkbox"/> Quinquenal | <input type="checkbox"/> Sem frequência definida |
|--------------------------------|-------------------------------|-------------------------------------|--------------------------------------------------|

**Q29** Quais foram as dificuldades principais que experimentaram na elaboração da AIN?

**Plano de Recuperação de Desastre (Disaster Recovery):****Q30** O hospital dispõe de um **Plano de Recuperação de Desastre**?☐ Sim☐ Não é Questão **Q34****Q31** Com que periodicidade revêem o Plano de Recuperação de Desastre?☐ Mensal☐ Bimensal☐ Trimestral☐ Semestral☐ Anual☐ Nenhuma**Q32** O Plano de Recuperação de Desastre tem as seguintes opções? (*pode seleccionar várias opções*)☐ Teste☐ Auditoria☐ Manutenção☐ Outros: \_\_\_\_\_**Q33** Como classifica os resultados definidos no Plano de Recuperação de Desastre e na Avaliação dos Riscos?☐ Bem definidos☐ Definidos minimamente☐ Pouco Definidos☐ Mal definidos**Q34** Qual a frequência com que efectua o *backup* dos dados?☐ Continua☐ Horária☐ Diária☐ Semanal☐ Mensal☐ Outra: \_\_\_\_\_**Q35** Como classifica a confiabilidade total dos *backups* actuais e os procedimentos de recuperação?☐ Muito confiáveis☐ Confiáveis☐ Pouco Confiáveis☐ Nada confiáveis**Q36** O hospital dispõe de técnicos habilitados a reagir imediatamente em caso de falha?☐ Sim☐ Não**Q37** O hospital dispõe, hoje, de *backup* de dados e um sistema de recuperação?☐ Sim☐ Não**Q38** Os *backups* de dados estão conservados no Datacenter?☐ Sim é Questão **Q40**☐ Não**Q39** Indique a solução para localização dos dados que escolheram?**Plano de Emergência:****Q40** O hospital dispõe de um Plano de Emergência?☐ Sim☐ Não é Obrigado. Terminou o questionário!**Q41** O Plano de Emergência contém a perspectiva☐ Interna☐ Externa☐ Ambas**Q42** Com que frequência são efectuados simulacros de situações de emergência?☐ Mensal☐ Trimestral☐ Semestral☐ Anual☐ Bianual☐ Não definida**MUITO OBRIGADO!**Se estiver interessado(a) em receber uma cópia do Relatório Final, envie um E-mail para: [vitor.vieira.alves@fe.up.pt](mailto:vitor.vieira.alves@fe.up.pt)

## **Anexo C – Standards Internacionais relacionados com BCM**

(Hiles 2007)

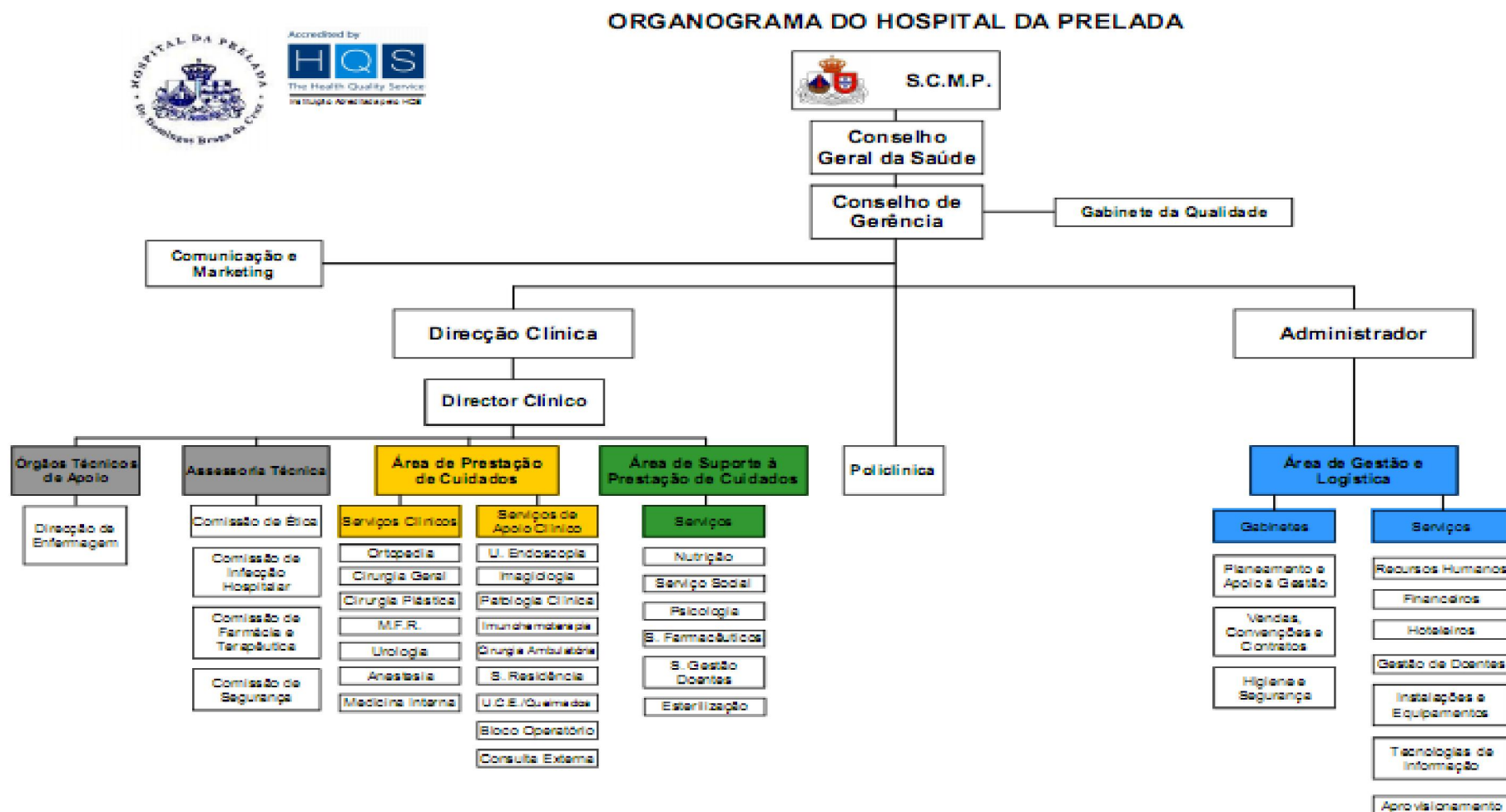
Pré 11 Setembro 2001

- Australia National Audit Office Best Practice Guide (Australia)
- American National Standards Institute / National Fire Protection Association ANSI/NFPA Standard 1600 (USA)
- British Standards Institution BS 7799 Information Security Standard (UK)
- DRII/BCI Common Body of Knowledge (USA and UK)
- Federal Emergency Management Agency (FEMA) Guidance Document (USA)
- Federal Financial Institutions Examination Council (FFIEC) BCP Handbook (USA)
- Office of Management and Budget (OMB) Circular A-130 (USA)
- Presidential Decision Directive 67 (USA)
- Turnbull Report (UK)

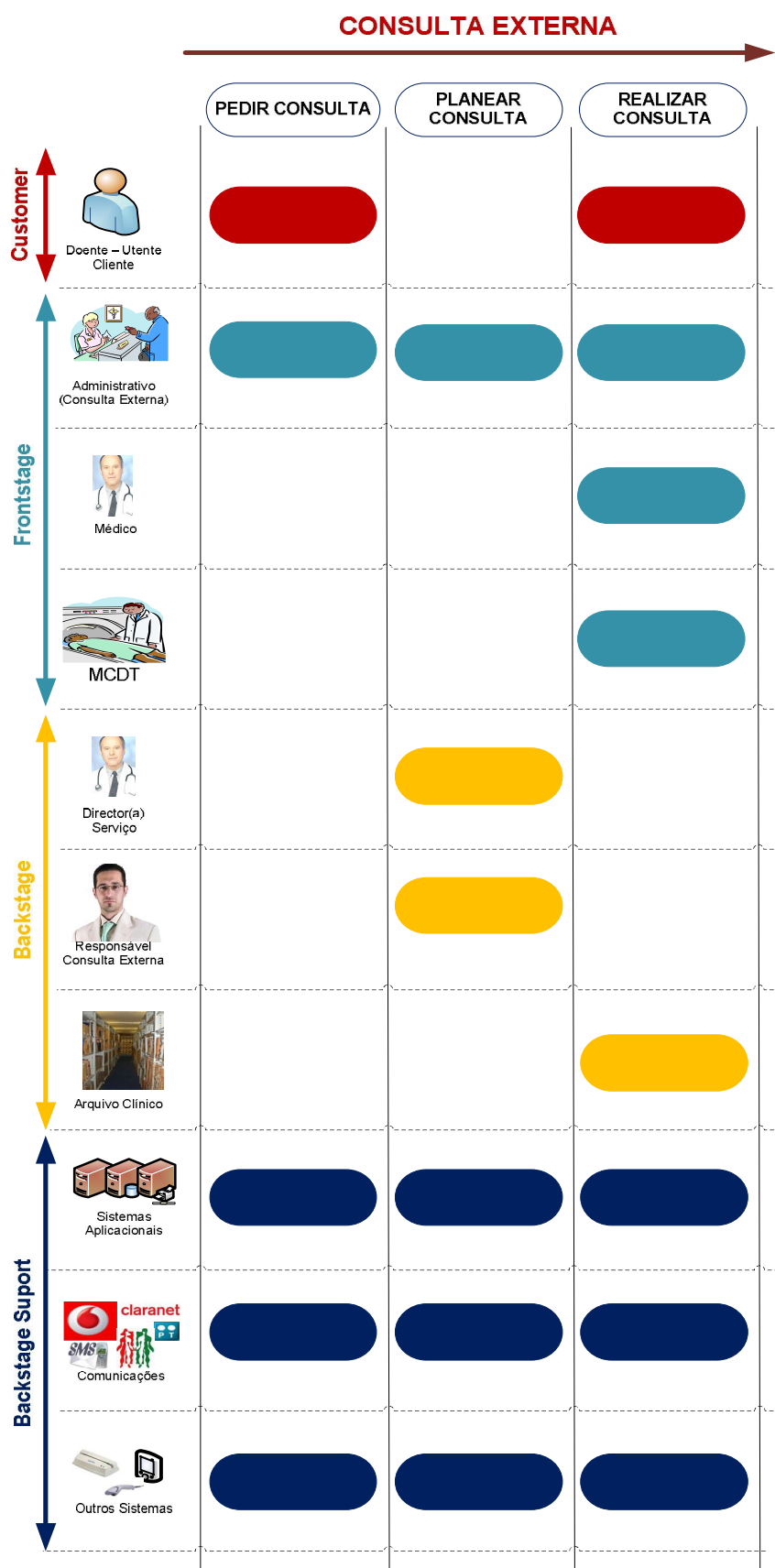
Pós 11 Setembro 2001

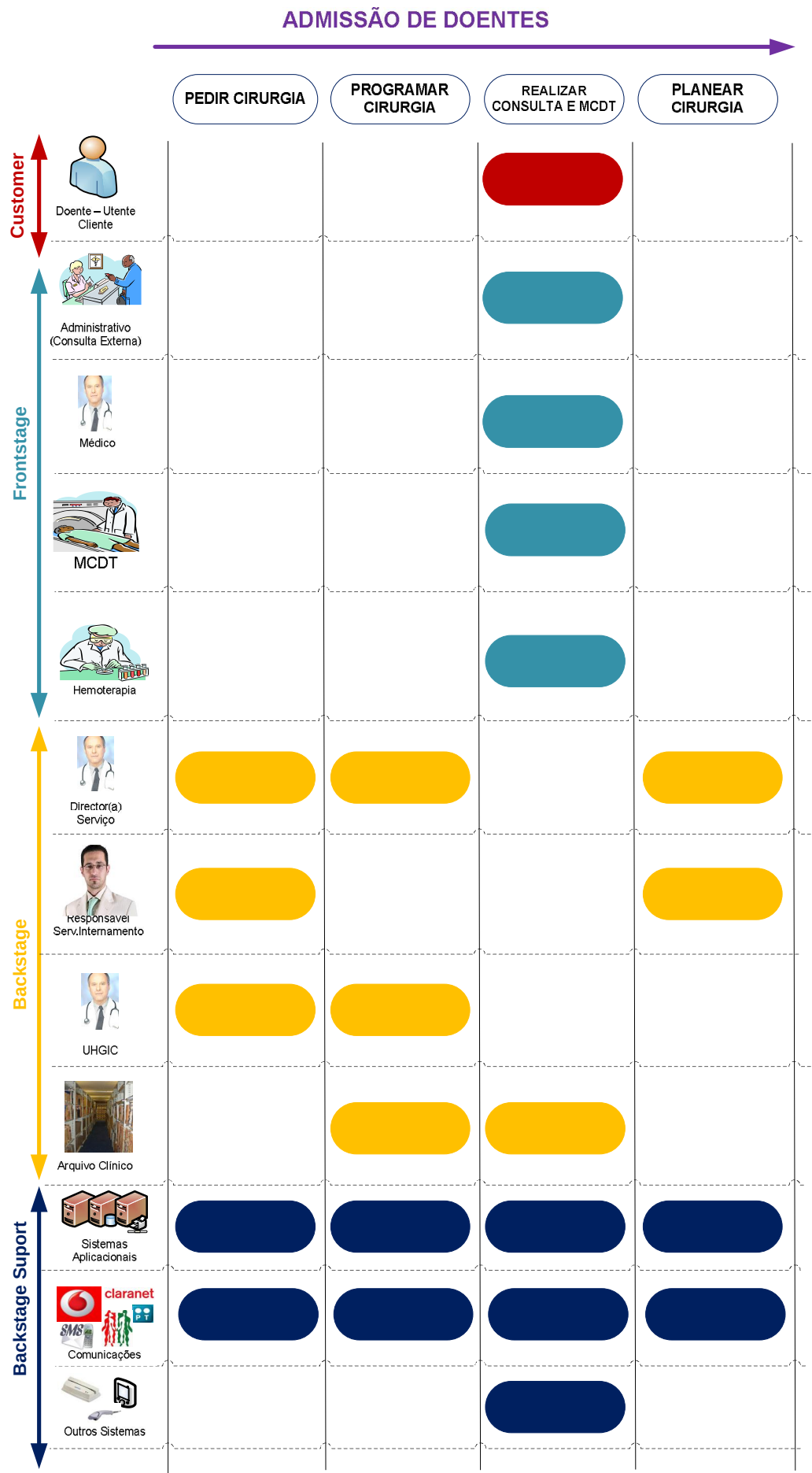
- Australia/New Zealand ANZ 4360: 2004 Risk Management
- Australia Standards BCM Handbook
- Bank of India BC Guidelines
- Bank of Thailand BC Guidelines
- Bank of Pakistan BC Guidelines
- Base Capital Accord (International)
- BSI/BCI Standard, PAS 56 (UK)
- BS 25999 Business Continuity Standard (UK)
- California Senate Bill SB 1386 (USA)
- Civil Contingencies Act (UK)
- Fair Credit Reporting Act (USA)
- Federal and Legislative BC Requirements for Internal Revenue Service (IRS) (USA)
- Federal Energy Regulatory Commission (FERC) Security Standards (USA)
- FFIEC BCP Handbook (USA)
- Board of Governors of Federal Reserve System; Office of the Comptroller of the Currency and Securities and Exchange Commission
- (FBR-OCC-SEC) Guidelines for Strengthening the Resilience of US Financial System (USA)
- Financial Services Authority (FSA) Handbook (UK)
- General Accounting Office (GAC) Potential Terrorist Attacks Guideline
- Health Insurance Portability and Accountability Act (HIPPA) Final Security Rule (USA)
- Information Systems Audit and Control Association (ISACA) Guidelines for BCP Audit (International)
- ISO 20000 (BS 15000) IT Service Management Standard (International)
- ISO/TS 16949 – The Harmonized Standard for the Automotive Supply Chain (International)
- Monetary Authority of Singapore (MAS) BCP Guidelines
- North American Industrial Classification System NAIC Standard on BCP (USA)
- NASD (National Association of Securities Dealers) Rule 3510 (USA)
- North American Electric Reliability Council (NERC) Security Guidelines (USA)
- National Futures Association (NFA) Compliance Rule 2-38 (USA)
- National Fire Prevention Association (NFPA) 1600 2004 (USA)
- National Institute of Standards and Technology (NIST) Contingency Planning Guide (USA)
- New York Stock Exchange (NYSE) Rule 446 (USA)
- Sarbanes-Oxley Act (USA)
- SS 507:2004 Singapore Standard for Business Continuity Disaster Recovery Service Providers
- BSI Publicity Available Specification 77 (PAS 77) IT Disaster Recovery Guidelines

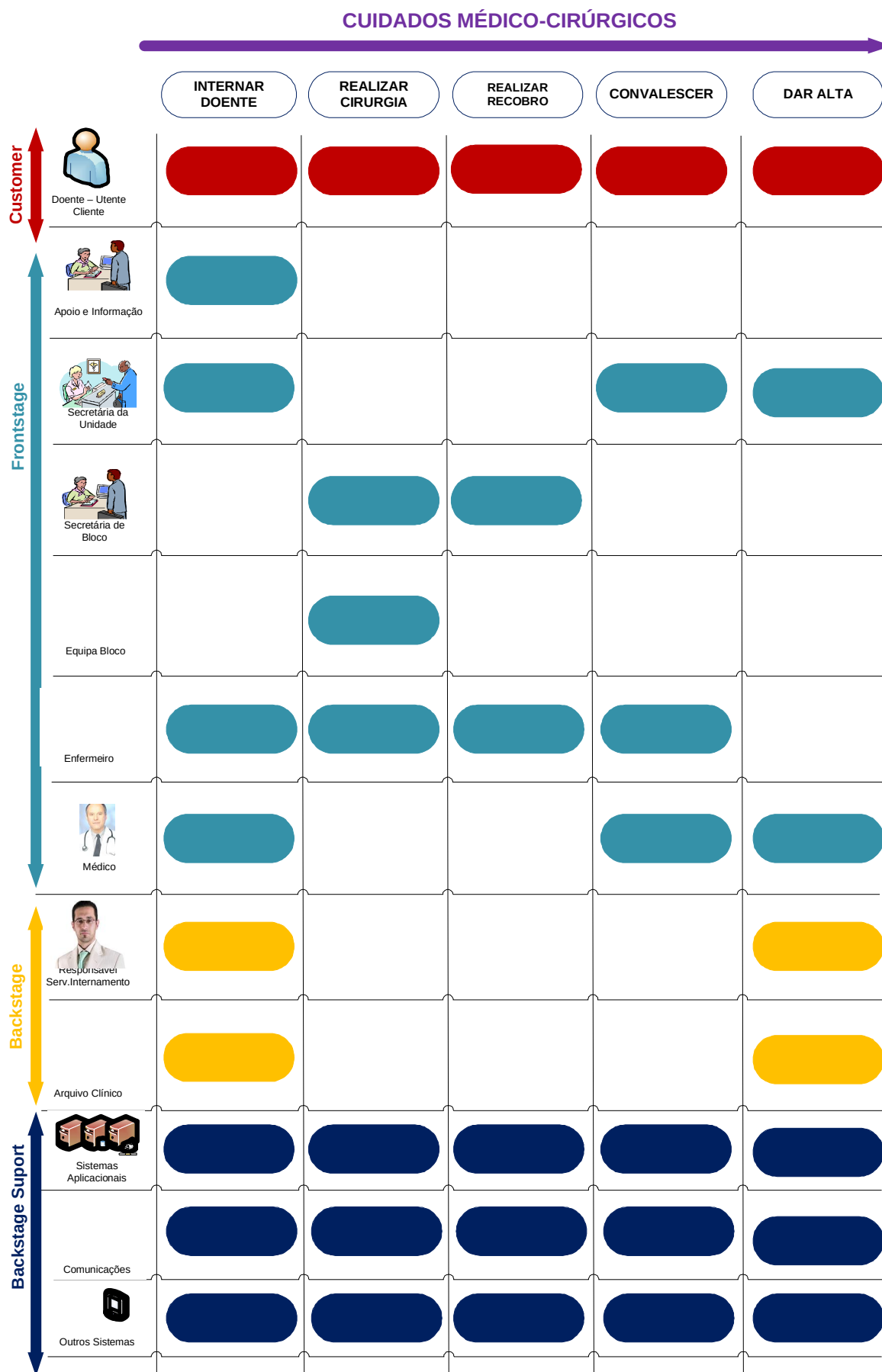
## Anexo D - Organograma do Hospital da Prelada Dr. Domingos Braga da Cruz



## Anexo E - Arquitectura do Sistema de Prestação de Serviço







## Anexo F – Processos de Negócio

| ÁREAS DE NEGÓCIO         |            | CONSULTA EXTERNA |                  |                   | ADMISSÃO DE DOENTES |                    |                          |                  | CUIDADOS MÉDICO - CIRÚRGICOS |                   |                  |             |          |
|--------------------------|------------|------------------|------------------|-------------------|---------------------|--------------------|--------------------------|------------------|------------------------------|-------------------|------------------|-------------|----------|
|                          |            | Direcção:        |                  |                   | Direcção:           |                    |                          |                  | Direcção:                    |                   |                  |             |          |
| UNIDADES DE NEGÓCIO      |            |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
| PROCESSOS DE NEGÓCIO     |            | Pedir Consulta   | Planear Consulta | Realizar Consulta | Pedir Cirurgia      | Programar Cirurgia | Realizar Consulta e MCDT | Planear Cirurgia | Internar Doente              | Realizar Cirurgia | Realizar Recobro | Convalescer | Dar Alta |
| ACTORES                  |            |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
| RECURSOS HUMANOS (Total) |            |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
| APLICAÇÕES INFORMÁTICAS  |            |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
| SISTEMAS TECNOLÓGICOS    | COM        |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
|                          | SERVIDORES |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |
|                          | OUTROS     |                  |                  |                   |                     |                    |                          |                  |                              |                   |                  |             |          |

## Anexo G - Análise de Impacto no Negócio – Processos – Questionário

## ANÁLISE DE IMPACTO NO NEGÓCIO

| PROCESSO                                                          |                                                                                                                                                                                         |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processo Principal:                                               | <b>PEDIR CONSULTA</b>                                                                                                                                                                   |
| Descrição do Processo:<br>(O que é que faz)                       | <b>Conjunto de actividades com o objectivo de registar os pedidos de consulta de especialidade por iniciativa dos utentes do SNS, de subsistemas de saúde e por iniciativa privada.</b> |
| Serviços Prestados:<br>(Descrição dos serviços que são entregues) | <b>Lista de pedidos de consulta por especialidade.</b>                                                                                                                                  |
| Importância do Processo:                                          | <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 (1-Não Crítico a 5 Muito Crítico)                |
| Área de Negócio:                                                  | <input type="checkbox"/> Consulta Externa <input type="checkbox"/> Admissão de Doentes <input type="checkbox"/> Cuidados Médico-Cirúrgicos                                              |
| Responsável:                                                      |                                                                                                                                                                                         |
| Importância na Área de Negócio:                                   | <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 (1-Não Crítico a 5 Muito Crítico):               |

| Unidade(s) de Negócio envolvidas no Processo           | Prioridade na UN         |                          |                          |                          |                          | Unidade(s) de Negócio envolvidas no Processo            | Prioridade na UN         |                          |                          |                          |   |
|--------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|---------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|---|
|                                                        | 1                        | 2                        | 3                        | 4                        | 5                        |                                                         | 1                        | 2                        | 3                        | 4                        | 5 |
| <input type="checkbox"/>                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Serviço Internamento          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Arquivo Clínico                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Análises Clínicas             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Hemoterapia                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Imagiologia                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Tratamentos Ambulatório        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Ortopedia 4                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Ortopedia 5                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Cirurgia Plástica / Queimados | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Cirurgia Geral e Urologia      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |
| <input type="checkbox"/> Oftalmologia                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> Medicina Física e Reabilitação | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |   |

O Processo gera proveitos:  
(Se SIM, estimar o valor anual dos proveitos)

☐ Não ☐ Sim

Valor anual dos Proveitos:

Cientes:  
(Quem são os clientes ou  
receptores dos serviços entregues  
pelo Processo.  
Podem ser internos e/ou externos.)

#### APLICAÇÕES UTILIZADAS:

- |                                                             |                                                     |                                                |
|-------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------|
| <input type="checkbox"/> Gestão Hospitalar                  | <input type="checkbox"/> Admissão de Doentes        | <input type="checkbox"/> Arquivo Clínico       |
| <input type="checkbox"/> PCE - Processo Clínico Electrónico | <input type="checkbox"/> Bloco Operatório           | <input type="checkbox"/> Consulta Externa      |
| <input type="checkbox"/> SIGLIC                             | <input type="checkbox"/> Facturação                 | <input type="checkbox"/> Indicadores de Gestão |
| <input type="checkbox"/> FACTUS                             | <input type="checkbox"/> Internamento / Ambulatório | <input type="checkbox"/> Registo de MCDTs      |
| <input type="checkbox"/> EDEIALAB                           |                                                     |                                                |
| <input type="checkbox"/> SIBAS                              |                                                     |                                                |

#### IMPACTO NO NEGÓCIO

Objectivos Temporais de Recuperação:  
(Quanto tempo pode o Processo estar inoperacional até impactar criticamente a unidade?)

Objectivos do Ponto de Recuperação:  
(Tempo de recuperação dos dados após o Processo estar operacional?)

Impacto em caso de falha do Processo: 0 – Sem impacto; 1 – Menor; 2 – Moderado; 3 – Muito; 4 – Crítico

| 0-3 h                | 3-6 h                | 6-12 h               | 12-24h               | 1 Dia                | 1 Sem                | 2 Sem                | 1 mês                | Tolerância Máxima    |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Impacto financeiro em caso de falha do Processo:

| 0-3 h                | 3-6 h                | 6-12 h               | 12-24h               | 1 Dia                | 1 Sem                | 2 Sem                | 1 mês                | Outras Despesas      |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Existem documentos alternativos ou manual de procedimentos? ☐ Não ☐ Sim

Localização dos Backups dos Dados:  
(Onde está localizada a informação de backup?)

Como recupera ou reescreve a informação perdida?  
(Passos para a recuperação da Processo após um evento)

**DEPENDÊNCIAS**

Quem e o que está dependente deste Processo?  
(Outras unidades de negócio dentro da Área de Negócio, outros  
sistemas que este Processo alimenta.)

**INPUT** (Informação que alimenta o processo)

Trabalho recebido - Interno e Externo:  
(De que forma este Processo recebe os inputs para iniciar?)

Origem:  
(Quem é a fonte dos inputs?)

Localização:  
(Onde estão localizados os inputs do processo?)

Como é recebido?  
(Descreva como o input é recebido e qual o método?)

Qual o impacto se não for recebido?  
(Qual o impacto se o input não for recebido?)

Opções:  
(Descreva os métodos de contornar a falta de informação para  
que o Processo continue,  
Ou se o Processo se atrasa devido à indisponibilidade dos inputs  
por um período de tempo.)

**OUTPUT** (Informação deste processo que alimenta o processo seguinte)

Trabalho entregue - Interno e Externo:  
(Que processo(s) recebe(m) o serviço entregue por este?)

Cliente:  
(Quem são os destinatários do serviço entregue?)

Localização:  
(Onde está localizada?)

Como é entregue:  
(Descreva como o output é entregue e qual o método?)

Qual o impacto se não for entregue?  
(Qual o impacto se o output não for entregue?)

Opções:  
(Descreva os métodos de contornar a falta para que o processo  
seguinte continue ou se o Processo se atrasa devido à  
indisponibilidade dos outputs por um período de tempo.)

## COLABORADORES

(Colaboradores responsáveis pela recuperação do Processo)

Colaborador Principal:  
(O principal responsável ou quem lidera o processo de recuperação.)

Colaborador Alternativo:  
(Quem substitui o responsável na condução do processo em caso de ausência.)

Formação:  
(Os colaboradores têm formação na recuperação da informação.)

☐ Não ☐ Sim

Qual o impacto se não estiver  
contactável?  
(Descreva o impacto se os colaboradores referidos não estiverem disponíveis)

Opções:  
(Descreva o que fazer se os colaboradores referidos não estiverem disponíveis.)

## PROVEITOS

Apresente uma estimativa dos Proveitos anuais gerados por este Processo

## OBSERVAÇÕES

Data:

Responsável Processo:

Data:

Serviço Tecnologias de  
Informação:

## Anexo H – Análise de Impacto no Negócio – Sistemas – Questionário

### ANÁLISE DE IMPACTO NO NEGÓCIO

#### Identificação das Tecnologias de Informação e Comunicação

|                                        |                                 |                          |                    |                |
|----------------------------------------|---------------------------------|--------------------------|--------------------|----------------|
| Área de Negócio:                       | <b>ADMISSÃO DE DOENTES</b>      |                          |                    |                |
| Processo:                              | <b>Realizar Consulta e MCDT</b> |                          |                    |                |
| <u><b>SI/TIC - Aplicações</b></u>      |                                 |                          |                    |                |
| <b>Aplicações</b>                      | <b>Plataforma</b>               | <b>Sistema Operativo</b> | <b>Criticidade</b> | <b>Suporte</b> |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
| <u><b>SI/TIC - Comunicações</b></u>    |                                 |                          |                    |                |
| <b>Função</b>                          | <b>Plataforma</b>               | <b>Sistema</b>           | <b>Criticidade</b> | <b>Suporte</b> |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
| <u><b>SI/TIC – Outros Sistemas</b></u> |                                 |                          |                    |                |
| <b>Função</b>                          | <b>Plataforma</b>               | <b>Sistema</b>           | <b>Criticidade</b> | <b>Suporte</b> |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |
| <u><b>Política de Segurança</b></u>    |                                 |                          |                    |                |
| <b>Periodicidade</b>                   | <b>Tipo de Segurança</b>        | <b>Suporte</b>           | <b>Localização</b> |                |
|                                        |                                 |                          |                    |                |
| <u><b>Teste de Segurança</b></u>       |                                 |                          |                    |                |
| <b>Efectuado</b>                       | <b>Periodicidade</b>            | <b>Falhas Detectadas</b> |                    |                |
|                                        |                                 |                          |                    |                |
| <u><b>Observações</b></u>              |                                 |                          |                    |                |
|                                        |                                 |                          |                    |                |

|              |  |                    |  |
|--------------|--|--------------------|--|
| <b>Data:</b> |  | <b>Assinatura:</b> |  |
|--------------|--|--------------------|--|

## Anexo I – Imagens da *Workshop* “Identificando Riscos, Construindo Alternativas”



## Anexo J – Matriz de Análise de Vulnerabilidades

| Evento               | Probabilidade |       |       |        | Risco         |                |           |       |       | Preparação |        |     | Total |
|----------------------|---------------|-------|-------|--------|---------------|----------------|-----------|-------|-------|------------|--------|-----|-------|
|                      | Alto          | Médio | Baixo | Nenhum | Ameaça à Vida | Ameaça à Saúde | Disrupção |       |       | Frac       | Normal | Boa |       |
|                      |               |       |       |        |               |                | Alta      | Média | Baixa |            |        |     |       |
| Pontuação            | 3             | 2     | 1     | 0      | 5             | 4              | 3         | 2     | 1     | 3          | 2      | 1   |       |
| Eventos Naturais     |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
| Eventos Tecnológicos |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
| Eventos Humanos      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |
|                      |               |       |       |        |               |                |           |       |       |            |        |     |       |

Fonte: Adaptado de American Society for Healthcare Engineering of the American Hospital Association