

UMA ABORDAGEM RELACIONAL E PLANEADA PARA A APLICAÇÃO DE
MODELOS DE GESTÃO DA SEGURANÇA NA SAÚDE

Por

RUI JORGE MEIRELES MACEDO CORREIA GOMES

Licenciado em Engenharia Electrotécnica

2010

Mestrado de Informática Médica

Faculdade de Ciências | Faculdade de Medicina

Universidade do Porto

UMA ABORDAGEM RELACIONAL E PLANEADA PARA A APLICAÇÃO DE
MODELOS DE GESTÃO DA SEGURANÇA NA SAÚDE

Tese Aprovada:

Professor Doutor Luís Velez Lapão

Professor Doutor Luís Filipe Coelho Antunes

À Sofia, Afonso e Rosário, uma
dedicatória especial com um pedido de
desculpas pelas memórias perdidas mas
que desejo recuperar na melhor
dimensão de pai e marido.

AGRADECIMENTOS

Gostaria de agradecer ao meu orientador, Professor Doutor Luís Velez Lapão, por todo o tempo que se deu à minha investigação, e como a sua força e persistência foram fundamentais para que eu pudesse concluir a dissertação. Um agradecimento também muito especial ao Prof. Doutor Luís Filipe Coelho Antunes, pela colaboração que deu com todas as valiosas sugestões e ao Departamento de Bioestatística da Faculdade de Medicina da Universidade do Porto, em nome do Prof. Doutor Altamiro da Costa Pereira e do Prof. Doutor Ricardo Correia que depositaram ímpar estímulo e confiança ao meu trabalho.

SUMÁRIO

A Segurança é um termo que transmite bem-estar e alguma tranquilidade principalmente a quem tira partido das suas propriedades. É difícil garantir a segurança sobre a perspectiva da gestão da informação disposta no formato convencional, ou em formato electrónico, e sujeita aos mais diversos meios de transmissão ou de armazenamento. A procura de um ambiente totalmente seguro é praticamente impossível, não só pelos custos exorbitantes que suscitaria mas também porque implicaria activar o controlo de todas as variáveis que integram o universo das vulnerabilidades, tais como as infra-estruturas físicas e lógicas, meios de acesso, pessoas, e outros recursos. A definição e padronização de métodos que ajudem, de uma forma global, a proteger um *bem* resultam geralmente de esforços das comunidades, muitas vezes compostas por entidades públicas e privadas em todo o mundo, que estabelecem documentos que padronizam, através de recomendações, uma boa gestão da Segurança. Esta dissertação estuda a possibilidade de se utilizarem alguns desses métodos, utilizando ferramentas que apoiam ao Governo das Tecnologias da Informação, no âmbito da gestão da Segurança da Informação e da sua preservação nas trocas de informação dentro e entre unidades de prestação de cuidados de saúde. O estudo pretende demonstrar também que a aposta na Segurança da Informação é um processo de gestão e não de tecnologias e que sistemas mais seguros não são sinónimos obrigatórios de processos mais lentos e caros.

ABSTRACT

Security means delivering tranquility and confidence for all involved. From an information management perspective, achieving a real security environment, covering information communication, processing and archiving needs, is a challenge. The demand for a totally safe environment is virtually impossible to be met. Expense grows exponentially when the aim is to monitor and control all variables and vulnerabilities related to logical and physical infrastructures, systems access, people and other resources. The establishment of standards and methods that effectively help support security efforts has been possible thanks to joint efforts by communities, public and private sectors. Globally necessary approaches to ensure organizational assets are protected are being developed into established management of information security standards and good practices. Thus, this thesis aims to provide a structured view of major *IT Governance* standards and tools in healthcare. Particularly looking into information security management and preservation and how it affects internal and external communications processes in health care organizations. The study also highlights that investment in information security is a management challenge rather than a technical issue and that safer systems are not synonymous of slower or more expensive ones.

PREÂMBULO

A (IN) SEGURANÇA NO ACESSO À INFORMAÇÃO

Nos últimos anos tem vindo a aumentar o número de instituições diferenciadas públicas e privadas que prestam serviços de apoio aos organismos de saúde com acessos legitimados à Rede da Informação da Saúde do Governo (RIS). A gestão da segurança da informação não tem sido uma prioridade. Segundo dados de 2004 da UMIC¹ relativamente aos Hospitais [1], 97% dos hospitais tem ligações à Internet, principalmente por banda larga (94%), com 38% a terem ligações com larguras de banda maiores ou iguais a 2 Mbps. Aproximadamente 17% dos hospitais com ligação à Internet disponibilizam acesso à rede aos doentes internados e 23% dos hospitais têm telemedicina, principalmente telediagnóstico e teleconsulta. É suficiente com estes indicadores perceber onde se poderão encontrar potenciais vulnerabilidades, provenientes do ambiente externo, se interrogarmos que níveis de segurança estão implementados na rede de dados da saúde, ou até nos ambientes internos quando se disponibilizam serviços de acesso à internet (com ou sem fios) aos funcionários, utentes e até mesmo as visitas dentro de organismos de saúde.

A sensação global de insegurança ao redor das TI (Tecnologias da Informação) é um tema sempre actual mas ao que parece com tendências de crescimento senão vejamos a aposta em mecanismos de segurança que grandes produtores de software como Microsoft, HP, Oracle, Google, entre outros, têm vindo a incluir nos produtos mais recentes que lançam no mercado. O aumento dos recursos informatizados faz aumentar a exposição ao risco que por consequência faz aumentar a complexidade nos mecanismos de protecção. Este aumento de complexidade leva-nos a concluir que já não é suficiente adoptar mecanismos de protecção mas que é necessário vigiar com permanência os riscos e otimizar constantemente esses mecanismos de protecção. É necessário *gerir a Segurança*.

¹UMIC: Agência para a Sociedade do Conhecimento. É o organismo público português com a missão de coordenar as políticas para a Sociedade da Informação.

A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Em Portugal encontram-se poucos estudos académicos ou da indústria com intenção de quantificar quais os níveis de adesão das empresas à utilização de modelos típicos para a gestão da segurança da informação. É normal encontrarem-se estudos que estão puramente focados no nível de adesão às TIC (Tecnologias da Informação e da Comunicação) - veja-se o exemplo do inquérito realizado pela UMIC à população portuguesa em 2003, e o estudo realizado por esta mesma entidade à Administração Pública [2], com o objectivo de recolher dados para perceber o nível de utilização das TIC em Portugal – e outros tipos de estudos que estudam indicadores da apetência das empresas e utilizadores à utilização de mecanismos tecnológicos de protecção tais como anti-vírus, *firewalls*, certificados digitais, entre outros mecanismos de segurança.

A partir dos resultados destes estudos onde, é explícito um considerável aumento do uso das TIC, e se assumirmos que esse aumento da utilização é directamente proporcional ao crescimento das vulnerabilidades nos ambientes em que são introduzidos, e tendo em conta que um processo de segurança da informação eficaz se deve iniciar sempre como um processo de gestão e só depois tecnológico, podemos questionar se todos os organismos, que têm os mecanismos de protecção tecnológicos da notoriedade tiveram antes de mais por base algum modelo de gestão com um plano e políticas de segurança para justificar e sustentar esse investimento tal como a capacidade de continuidade nessa gestão. Ou simplesmente, diligenciaram uma ou duas medidas que se prestam exclusivamente a mitigar ameaças externas, a nível de circulação de informação electrónica, como os anti-vírus, *firewall* e certificados digitais.

Segundo um relatório elaborado pela Symantec em 2007 sobre as ameaças que as empresas estão sujeitas a partir da *internet* apresenta dados relativos ao segundo semestre de 2006 [3], no qual indica que houve um crescimento acentuado de ameaças ao comércio electrónico. Os ataques contra tecnologias que utilizem aplicações de *internet* estão cada vez mais populares, o espaço de tempo entre a vulnerabilidade e o ataque é cada vez mais curto, existiu um crescimento acentuado das redes informáticas e um aumento das vulnerabilidades graves (fáceis de explorar). O roubo de identidade é um problema de segurança cada vez mais frequente. As organizações que armazenam e gerem informações de identificação pessoal têm de adoptar medidas para garantir a confidencialidade e a integridade desses dados. Qualquer

problema que resulte na fuga de dados de identificação pessoal pode dar origem à perda de confiança pública, a responsabilidade jurídica e/ou a litígios dispendiosos. Por isso em Julho de 2006, através do Decreto-Lei nº 116-A/2006, o governo português decidiu dar luz verde à criação de um Sistema de Certificação Electrónica do Estado – Infra-Estrutura de Chaves Públicas (SCEE) para disponibilização de assinaturas electrónicas para as entidades públicas e para os serviços e organismos da Administração Pública ou outras entidades que exerçam funções de certificação no cumprimento de fins públicos. Estas entre outras iniciativas são relevantes quando consideradas ameaças de proveniência externa, nomeadamente através da *internet*. No entanto se enumerarmos as ameaças que as organizações internamente também enfrentam quando sujeitas a uma má gestão dos recursos por parte do Departamento de Sistemas de Informação (DSI) ou de outras estruturas hierárquicas, quando por exemplo existem partilhas das credenciais entre utilizadores, falta do controlo dos acessos físicos e lógicos aos centros de dados, até ao mau planeamento e falta de arquitectura na introdução de projectos de infra-estruturas físicas e tecnológicas.

O ELO MAIS FRACO

As acções ou actos de negligência dos colaboradores das empresas são considerados uma das principais ameaças à segurança informática das organizações. A precariedade com que muitas vezes são delegadas as funções de administração e/ou manutenção de sistemas e havendo cada vez maior conhecimento por parte dos utilizadores, sobre o manuseamento dos computadores, dos sistemas operativos e de base de dados leva a que as potenciais falhas de segurança estejam localizadas no interior das organizações que estão sujeitas a este *elo mais fraco*. Entre essas ameaças está por vezes o acesso físico e lógico facilitado a pontos nevrálgicos como o centro de dados, zonas de arquivos, ao bastidor de comunicações a pessoas não autorizadas. Esta preocupação já tem vindo a levar algumas organizações a tomar a iniciativa de implementar práticas de gestão da segurança de forma alinhada com a estratégia da organização de modo a serem capazes de mitigar as vulnerabilidades internas e tirar os melhores proveitos dos investimentos nas TI. Desde as burlas típicas informáticas, à invasão da vida privada, acesso ilegal a dados, falsificações de cartões, burlas de telecomunicações, acidentes, etc. o risco de possuir uma infra-estrutura não segura é enorme. As organizações necessitam de reduzir os

riscos inerentes ao uso das infra-estruturas de TI e simultaneamente obter indicadores de benefícios que permitam sustentar o investimento numa infra-estrutura segura.

MODELOS PARA APOIAR A INDÚSTRIA E A SAÚDE

Critérios de como garantir a confidencialidade dos dados de saúde dos utentes, identificação de dadores de órgãos, acessos físicos, acessos lógicos, etc., deveriam estar sujeitos a restrições que tivessem em consideração um rigoroso sistema específico de gestão de segurança. A norma de certificação da segurança, ISO/IEC 27001², publicada pela *International Standardization Organization* (ISO)³ em 2005, pode ser utilizada em qualquer indústria, por ser suficientemente flexível e abrangente e o modelo de boas práticas para a saúde homologado em Julho de 2008, ISO 27799⁴, estão perfeitamente alinhados como modelos de gestão típicos, tal como se encontram na Qualidade e Ambiente respectivamente ISO 9001⁵ e ISO 14000⁶, e apresentam-se como plataformas de gestão que podem endereçar por completo a necessidade de um conjunto de boas práticas e de um modelo de gestão relativamente à segurança da informação existente nos organismos de saúde.

² ISO/IEC 27001/2005: *Information technology - Security techniques - Information security management systems*.

³ ISO: *International Standardization Organization International Standards for Business, Government and Society*. www.iso.org

⁴ ISO 27799/2008: *Health informatics -- Information security management in health using ISO/IEC 27002*

⁵ ISO 9001/2000: *Quality management systems -- Requisitos para um sistema de Qualidade*

⁶ ISO 14000/2006: *Environmental management -- Environmental communication*

Japan	3378	Slovenia	13
India	484	France	12
UK	407	Netherlands	12
Taiwan	386	Saudi Arabia	12
China	251	Pakistan	11
Germany	135	Bulgaria	10
Korea	106	Norway	10
USA	95	Russian Federation	10
Czech Republic	85	Kuwait	9
Hungary	66	Sweden	9
Italy	58	Slovakia	8
Poland	40	Bahrain	7
Spain	39	Colombia	7
Austria	32	Indonesia	7
Hong Kong	31	Iran	7
Australia	29	Croatia	6
Ireland	29	Switzerland	6
Malaysia	27	Canada	5
Mexico	26	South Africa	5
Thailand	26	Sri Lanka	5
Greece	25	Lithuania	4
Romania	25	Oman	4
Brazil	23	Qatar	4
Turkey	20	Portugal	3
UAE	18	Outros	50
Philippines	15		
Iceland	14		
Singapore	13	Total	6099

Número de certificados ISO/IEC 27001 por país[4]⁷

⁷ Disponível em <http://www.iso27001certificates.com>. Acedido a 20/04/2010.

ÍNDICE

AGRADECIMENTOS	v
SUMÁRIO	vi
ABSTRACT.....	vii
PREÂMBULO.....	viii
ÍNDICE	xiii
ACRÓNIMOS	xvi
ÍNDICE DE FIGURAS.....	xvii
ÍNDICE DE TABELAS.....	xix
ORGANIZAÇÃO DA TESE	xx
RESULTADOS CIENTÍFICOS	xxii
1. INTRODUÇÃO.....	23
1.1. Considerações e problemas a endereçar.....	24
1.2. Motivações para a Investigação	26
1.3. Metodologia de investigação	31
2. PRIVACIDADE & ACESSO À INFORMAÇÃO CLÍNICA	33
2.1. Contexto da Informação	33
2.2. Contexto da Segurança.....	35
2.3. Níveis de Maturidade da Informação Clínica e a Segurança	40
2.4. Regulamentos.....	42
3. ESTRUTURA E GOVERNO DAS TI	43
3.1. Governo das TI.....	43
3.2. Governo nas organizações em geral.....	51
3.3. Governo nas organizações de saúde.....	53
3.4. A segurança das TI como habilitador de negócio	54
3.5. Análise de Risco.....	58
4. DEFINIÇÃO E EXPOSIÇÃO DO PROBLEMA	61
4.1. Exposição de contexto	61

4.2.	Questões a problemas localizados.....	62
5.	ARQUITECTURA EMPRESARIAL E SOCIAL	63
5.1.	Modelo de Actuação	63
5.2.	Do caos à estrutura.....	64
5.3.	Lidar com a complexidade.....	65
6.	INFRA-ESTRUTURAS E PROBLEMAS COMUNS DOS HOSPITAIS DO SNS	73
6.1.	Metodologia de Investigação	73
6.2.	Modelo de camadas.....	74
6.3.	Levantamento empírico de problemas mais comuns	76
7.	ELABORAÇÃO DE ESTRATÉGIAS PARA A RESOLUÇÃO DE PROBLEMAS	77
7.1.	Disponibilizar e proteger a informação de saúde.....	77
7.2.	Visão generalizada das normas	78
7.3.	Estratégias para a resolução de problemas.....	86
8.	APLICAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)	99
8.1.	O modelo PDCA (Plan-Do-Check-Act).....	99
8.2.	A estrutura do SGSI	101
8.3.	Processo de desenvolvimento de um SGSI	102
9.	ESTUDO DE CASO	108
9.1.	Introdução	108
9.2.	Caracterização do hospital	108
9.3.	Estudo 1 – Gestão da Segurança	109
9.4.	Estudo 2 – Gestão de Serviços de TI	115
9.5.	Conclusões	121
10.	ENSAIO DE RESPOSTA AOS PROBLEMAS COLOCADOS.....	124
10.1.	Interpretação dos Resultados	124
10.2.	Ensaio de resposta aos problemas colocados	125
10.3.	Tendências e Investigação de futuro	127
11.	CONCLUSÕES.....	130
	GLOSSÁRIO	132
	BIBLIOGRAFIA	134
	ANEXO A.....	139

ANEXO B..... 147

ANEXO C..... 157

ANEXO D..... 164

ACRÓNIMOS

BSI	British Standards Institute
CEN	CEN - Comité Européu de Normalização
CEO	Chief Executive Officer
CIO	Chief Information Officer
Ciso	Chief Information Security Officer
Cobit	The Control Objectives for Information and related Technology
CT	Comissão Técnica Portuguesa de Normalização
DSI	Departamento de Sistemas de Informação
PCE	Processo Clínico Electrónico
ERP	Enterprise Resource Planning
ISO	International Organization for Standardization
Ncsc	National Computer Security Center
Nist	National Institute of Standards and Technology
NP	Norma Portuguesa
NSA	National Security Agency
RIS	Rede de Informação da Saúde
SNS	Serviço Nacional de Saúde Português
TI	Tecnologias da Informação
TIC	Tecnologias da Informação e da Comunicação

ÍNDICE DE FIGURAS

Figura 1: Dimensões da informação. Adaptado de <i>Jens-Erik Mai</i>	35
Figura 2: dimensões da segurança da informação	36
Figura 3: Confidencialidade dos dados	36
Figura 4: Integridade dos dados	37
Figura 5: Disponibilidade dos dados	37
Figura 6: A Segurança da Informação como um problema de negócio	39
Figura 7: Os 6 níveis de maturidade da informação clínica, adaptado <i>ICT Strategy 2007-2011</i> ...	41
Figura 8: <i>Framework IT-Governance 38500</i>	45
Figura 9: <i>IT-Governance</i> e Negócio, Adaptado a partir de modelo da ISACA	48
Figura 10: Teoria de controlo moderno (modelo com compensação)	49
Figura 11: Basic Control Loop	50
Figura 12: comportamento do controlo de um sistema ao longo de um tempo	50
Figura 13: Benefícios expectáveis do <i>IT-Governance</i>	52
Figura 14: Oportunidades relacionadas com a gestão da segurança	54
Figura 15: Exemplo de áreas a endereçar nas políticas da segurança.....	57
Figura 16: opções para tratamento do risco	59
Figura 17: modelo de avaliação de riscos	60
Figura 18: Cláusulas de segurança da ISO 27001.....	63
Figura 19: Os níveis de maturidade de um CIO	70
Figura 20: Inquérito às quebras de segurança “ <i>Information security breaches survey 2006</i> ” (PWC, Microsoft, Symantec, Entrust, ClearSwift).....	71
Figura 21: Níveis de Maturidade do Sistema de Informação Hospitalar	74
Figura 22: Exemplo da arquitectura típica de um ambiente de Informação Hospitalar do SNS..	75
Figura 23: Nível de risco pela exposição de informação por sector de actividade [30].....	77
Figura 24: Estrutura da ISO (<i>International Standardization Organization</i>).....	82
Figura 25:Estrutura da ISO/TC 215 <i>Health Informatics</i>	85
Figura 26: Estrutura típica de um governo para as TI numa organização.....	87
Figura 27 : Estrutura típica de um governo numa organização.....	88

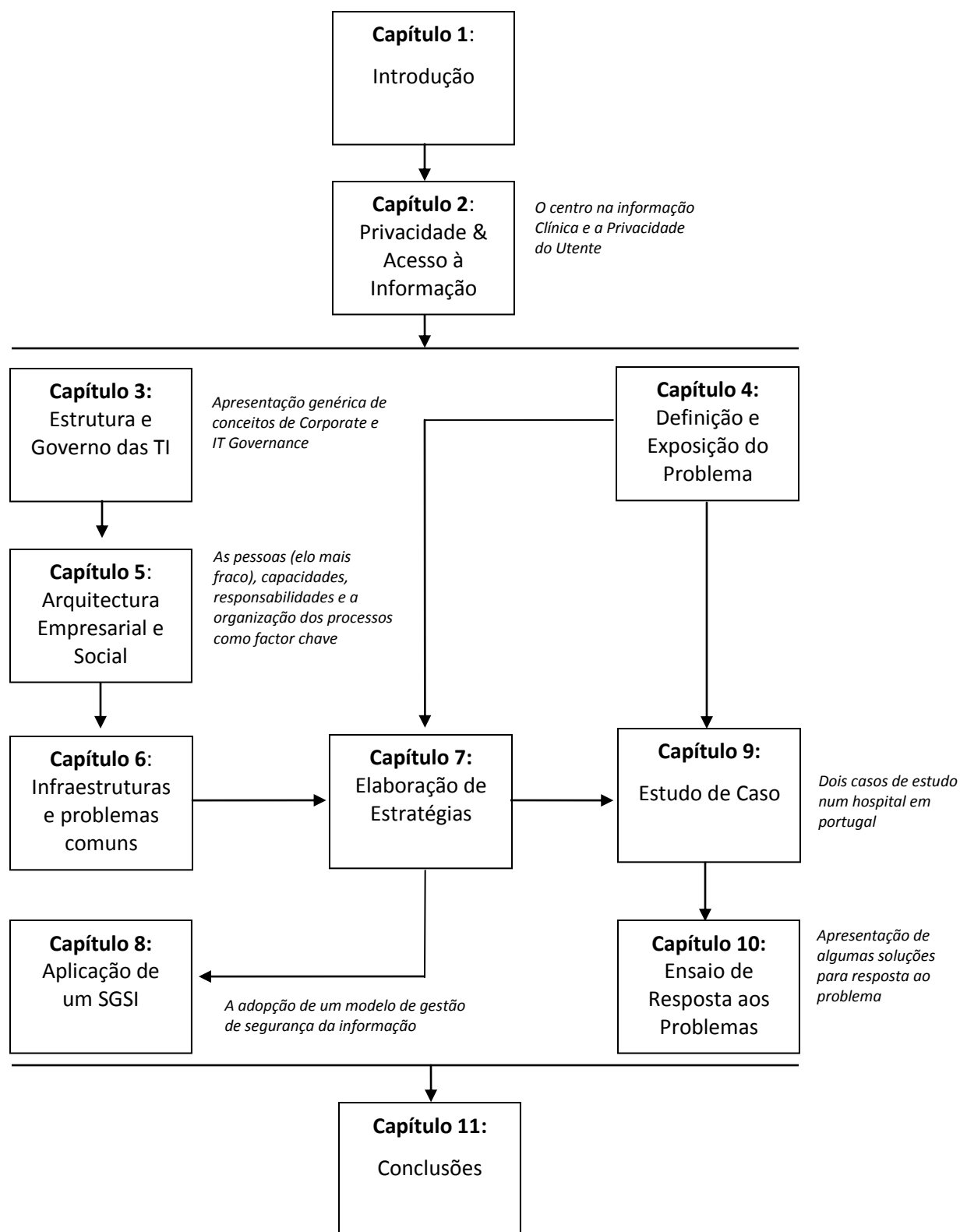
Figura 28: Origem da norma certificadora da segurança para a Saúde.....	91
Figura 29: Estrutura de um SGSI.....	93
Figura 30: Métricas do SGSI (composição da ISO/IEC 27000)	94
Figura 31: Exemplo de metodologia para uma <i>Gap Analysis</i>	97
Figura 32: Ciclo de desenvolvimento, manutenção e melhoria	100
Figura 33: Estrutura de um SGSI	101
Figura 34: Desenvolvimento de um SGSI segundo a ISO 27001	103
Figura 35: Cálculo de risco - antes e após a aplicação de controlos de segurança	106
Figura 36: Impacto do risco sobre os bens da organização (adaptada da ISO 27799)	107
Figura 37: Processo de <i>Gap Analysis</i>	111
Figura 38: Exemplo de matriz RACI.....	117
Figura 39: Aproximação a um modelo de cadeia de valor dos SI/TI do hospital.....	117
Figura 40: Nível de maturidade <i>IT Service Management</i>	119
Figura 41: <i>Incident Management Maturity Framework (PMF)</i>	120
Figura 42: modelo RACI de funções e responsabilidades.....	121
Figura 43 : Ferramenta ENISA para comparações diferentes métodos de Gestão de Risco.....	126
Figura 44: “2008, <i>Annual Output Statement</i> ”. Departamento de agricultura da União Europeia	128

ÍNDICE DE TABELAS

Tabela 1: Cenário real adaptado ocorrido num hospital em 2001	28
Tabela 2: Cenário de condições iniciais.....	30
Tabela 3: Classificação Funcional de Terminologias de Informática Médica	86
Tabela 4: Benefícios mais comuns das <i>framework</i>	88
Tabela 5: Benefícios mais comuns associados à ISO/IEC 27002 (ISF)	89
Tabela 6: Cláusulas de controlo na norma ISO/IEC 27002:2005	92
Tabela 7: Cláusulas para as boas práticas da ISO/IEC 27002.....	110
Tabela 8: Níveis de risco e áreas de actuação	112
Tabela 9: Pontos críticos (cláusula 3).....	113
Tabela 10: Pontos críticos (cláusula 5).....	113
Tabela 11: Pontos críticos (cláusula 6).....	114
Tabela 12 : Pontos críticos (cláusula 7)	115
Tabela 13: Comparação entre os dois modelos de gestão.....	122

ORGANIZAÇÃO DA TESE

Este trabalho está dividido em onze capítulos, para além de um preâmbulo, acrónimos, glossário, referências bibliográficas e quatro anexos. A introdução no primeiro capítulo apresenta uma descrição do objecto de estudo, os objectivos gerais e intermédios bem como a motivação. No capítulo segundo referencia-se a Informação de Saúde e a Privacidade do Doente como o elemento mais precioso no qual se centra toda a investigação com vista a proteger esse bem. O capítulo três aborda o governo das TI, o conceito de *Governance*, evolução e a sua pertinência no âmbito deste trabalho. Algumas definições da arquitectura empresarial e social, encarados de uma forma pessoal, podem ser consultadas de forma isolada no capítulo cinco. Os capítulos quatro, seis e sete exploram respectivamente a definição e exposição do problema, uma descrição das arquitecturas dos SI dos hospitais e a elaboração de estratégias para a resolução de problemas, no qual se dá especial ênfase às normas nacionais, europeias e internacionais. O capítulo 8 está estruturado de modo que se percebam onde ligam todos os elementos relevantes numa implementação de um Sistema de Gestão de Segurança da Informação (SGSI) e no capítulo 9 aproxima-se dois casos de estudo com implementações reais, de métodos orientados ao *IT Governance*, num hospital público. Finalmente nos Capítulos 10 e 11 pretende-se responder às questões colocadas nos capítulos anteriores e sistematizar o que poderia vir a ser um trabalho de investigação mais profundo.



RESULTADOS CIENTÍFICOS

(ANEXO C):

Gomes, R. J., Lapão, L.V. et al. (2008). "The Adoption of IT Security Standards in a Healthcare Environment." eHealth Beyond the Horizon – Get IT There S.K. Andersen et l. (Eds.) IOS Press, MIE 2008

(ANEXO D):

Lapão, L. V., Rebugue, A., Silva, M.S., Gomes, R. J. " ITIL Assessment in a Healthcare Environment: The Role of IT Governance at Hospital São Sebastião". Medical Informatics in a United and Healthy Europe K.-P. Adlassnig et al. (Eds.). IOS Press

CAPÍTULO I

1. INTRODUÇÃO

Num mundo em crescimento e demasiado competitivo, só mesmo as empresas que tiram partido do melhor que a informação pode disponibilizar, de base para a decisão podem contar com lucros e prosperar [5]. As organizações devem compreender que a informação é um recurso de tal forma valioso que deve ser protegido e gerido convenientemente. A segurança da informação deve ser utilizada como uma forma de proteger a informação contra o extravio, exposição ou destruição das suas propriedades. Um dos objectivos da segurança da informação é, assegurar a continuidade de negócio minimizando o impacto de incidentes de segurança.

A dependência que as organizações têm actualmente das infra-estruturas das TIC e que estão directamente associadas ao sucesso do seu negócio com todos os proveitos mas também com os riscos de exposição, exige das organizações a capacidade de uma gestão adequada no que respeita à Segurança da Informação. Um estudo a nível mundial publicado em Janeiro de 2008 pela *Delloite* [6] revela a necessidade de um reforço do investimento em segurança e privacidade para os próximos anos. Segundo esse estudo as empresas de tecnologias, multimédia e comunicações deverão reforçar de imediato os seus esforços e investimentos em segurança. As conclusões do estudo mostram que estas empresas já teriam de ter tomado medidas de forma a estarem preparadas para enfrentar uma eventual crise de segurança a partir de 2009. Durante os 2 meses que antecederam o inquérito a maior parte das empresas afirmam ter conseguido evitar uma importante crise de segurança, sendo que 69% dos inquiridos afirmam estar “muito confiantes” ou “extremamente confiantes” quanto à capacidade das respectivas empresas de enfrentar os desafios de segurança vindos do exterior.

Contudo, apenas 56% se mostra confiante relativamente à capacidade de se proteger no futuro das ameaças internas. Em Portugal, este tema parece também ser sempre de grande actualidade e consideração, até porque é comum algumas sensibilidades das empresas e dos media despertarem com meios de marketing tão-somente os além fronteiras vocabulários associados às TI tais como, *anti-virus*, *anti-spam*, *firewall*, *IT-Governance*, e como também é comum verem-se iniciativas de sensibilização, e *workshops* onde se debatem os temas.

1.1. Considerações e problemas a endereçar

Durante o período que compreendeu este estudo houve um esforço na procura de matéria que permitisse perceber qual a amplitude do problema da falta da segurança nas organizações em Portugal, nomeadamente nas prestadoras de cuidados de saúde, e no caso das implementações existentes que tiveram objectivos claros de mitigar o risco, procurar saber quais os padrões de medida que foram, ou deveriam ter sido, utilizados e que permitiram perceber qual o retorno e os requisitos mínimos que se conseguiram satisfazer. A principal constatação desta análise, retirada de forma percepcionada, foi verificar a completa ausência de qualquer certificação num modelo de gestão ou de serviços nas empresas e organismos de saúde em Portugal. A segunda impressão é que em termos de boas práticas e metodologias que ajudam nessa implementação também não é comum serem utilizadas. Nos hospitais do SNS as questões relacionadas com a interoperabilidade ou com a gestão de níveis de serviço têm sido muito mais opulentas do que propriamente a segurança uma vez que as acções que esses estudos transparecem ter muito pouco retorno à organização. Apostar na segurança e na sua gestão pode significar a introdução de latência na execução de serviços de rede ou servidores e também a necessidade de alocação de recursos humanos na documentação e organização de processos. É portanto uma aposta que tem custos de exploração directos e que não evidencia para uma administração potenciar qualquer lucro económico. Quanto aos directores dos DSI (departamentos de Sistemas de Informação) a percepção também não é favorável uma vez que por regra os gestores das TIC só acreditam ser possível beneficiar em simultâneo de dois dos três indicadores, *fast*, *cheap and secure* [7], e portanto a segurança acaba por poder significar sinónimo de sistemas mais lentos e/ou processos mais caros.

A amplitude do problema é mais perceptível para quem teve oportunidade de exercer durante anos uma gestão que vai desde a microinformática, gestão de projectos até à estratégia das TI

num organismo de saúde e teve oportunidade de aferir no terreno as dificuldades subjacentes ao governo das TIC. Com esse tipo de vivência foi possível perceber no local as dificuldades que os operacionais encontram na gestão das suas tarefas, a começar na gestão de níveis de serviços, organização do seu posto de trabalho até a conhecer o verdadeiro potencial e estrangulamentos existentes nos recursos disponíveis a essa actividade (humanos, físicos, logísticos e de software). Em complemento, beneficiar de uma visão de perspectiva macro permitiu também perceber qual o nível de alinhamento que deveria existir entre a estratégia definida para as TI e os interesses e objectivos da gestão.

Em Julho de 2007 a *European Network and Information Security Agency* ENISA⁸ [8] publicou um relatório designado “Prática Corrente e Avaliação do Sucesso Julho de 2007” com os resultados das iniciativas de sensibilização para a segurança da informação onde foram inquiridas organizações e organismos públicos europeus. Esse estudo apresenta resultados no qual se reconhece claramente que a maior preocupação das organizações e organismos públicos, no que respeita aos riscos por falta de segurança é a difusão de correio electrónico associado à potencial vulnerabilidade a vírus informáticos. Por outro lado a questão que menos ou nada preocupa os gestores desses organismos são as “políticas de secretária”. Assim, ao longo deste estudo espera-se que o leitor perceba, qual o impacto que tem, nas políticas e estratégias orientadas à gestão segurança, o que representa o valor desse indicador da secretária “arrumada” no sucesso ou insucesso da aplicação das boas práticas no âmbito da gestão da segurança da informação nas organizações.

1.1.1. Objectivos Gerais

É comum encontrarem-se estudos que correlacionam metodologias distintas de gestão e controlo das TIC utilizando as mais variadas normas contribuindo, por vezes, para alguma confusão a qualquer gestor de TIC ou executivo que procure cultivar-se no desenvolvimento do tema. O objecto deste estudo é proporcionar uma descrição generalizada de conhecimentos e apresentar uma estrutura de princípios para os governo das TI, com principal incidência nas normas de gestão da segurança da informação, no contexto da indústria em geral, apresentando as principais características de cada um deles, como se correlacionam, e as metodologias e

⁸ ENISA: Agência Europeia para a Segurança das Redes e da Informação é uma agência da União Europeia criada para fomentar o funcionamento do Mercado Interno. A agência tem como missão atingir um nível elevado e efectivo de segurança das redes e da informação na União Europeia.

normas de referência em que se assentam, e como poderiam vir a ser utilizados na área da saúde.

1.1.2. Objectivos Específicos

Para atingir esse objectivo esta investigação propõe a elaboração e referenciação de documentação suportada em normas, matrizes e tabelas de referência que:

- Proporcionem aos responsáveis pelas TIC dos hospitais uma visão simplificada das normas mais importantes que respeitam à gestão da segurança da informação;
- Apresentem indicadores de benefícios de se possuir uma infra-estrutura segura, nomeadamente para a gestão da informação clínica, e procurar a aplicabilidade das normas e métodos num cenário real;
- Sirvam como ponto de partida para uma *framework* para a saúde que permita em primeira instância apoiar a gestão da infra-estrutura das TI num controlo eficaz dos recursos e processos e apresentar um conjunto de regras, baseadas na estrutura de uma norma internacional ou europeia, que devidamente sistematizadas ajudam a retratar o estado da sua organização em matéria da segurança da informação;
- Ajudem a mostrar as vantagens que se obtêm quando na altura do planeamento estratégico das TI são conhecidos os riscos relacionados com a infra-estrutura TIC existente.

1.2. Motivações para a Investigação

1.2.1. Reconhecimento do Comité “Olímpico”

Dentro de qualquer sistema de saúde embora seja comum produzir-se e disponibilizar-se uma extensa quantidade de dados em suporte físico e electrónico que resultam de actividade de negócio de prestação de cuidados. Não é fácil controlar a existência tanto dos recursos afectos como as infra-estruturas de suporte a essa actividade. Gerir a segurança é uma actividade que é presumível existir, e é transversal a todos os sectores da organização. Nos hospitais do SNS particularmente esta actividade é de pouco comprometimento seja pela maior parte dos responsáveis das TIC como pelos executivos dos hospitais e daí o hábito de não incluir esta

temática nos planos de actividades dos serviços, e muito menos nomear agentes internos ou externos para apoiar o processo. Entre esses agentes, deveria haver uma entidade externa independente que ajuda-se no controlo e auditoria de processos de segurança. No entanto, o mais importante é conseguir estabelecer um comité nomeado internamente com o intuito de gerir a segurança da informação. O comité “olímpico”, ou mais propriamente o Comité da Segurança, que é atribuído a uma *taskforce* interna, é a primeira e a principal medida de demonstração de interesse do organismo em investir nesse processo. Esse grupo deve ter a participação activa de um sénior das TIC, que terá de ter funções exclusivas, e a tempo inteiro, de gestor da segurança (*Chief Information Security Officer-CISO*), mas também a presença de um vogal que faça parte do conselho de administração para que no mínimo viabilize formalmente o comprometimento do organismo no projecto e se responsabilize pelas medidas “olímpicas” a adoptar.

1.2.2. A “teoria” do caos na gestão das TIC

A Teoria do Caos apresenta a imprevisibilidade como a característica fundamental dos fenómenos complexos. Os fenómenos ditos “caóticos” são aqueles onde não há previsibilidade. O *efeito borboleta*⁹ foi abordado pela primeira vez em 1963 por *Edward Lorenz*, no qual segundo a teoria apresentada, o bater de asas de uma simples borboleta poderá influenciar o curso natural das coisas e, assim, talvez provocar por exemplo um furacão do outro lado do mundo. Acreditando na autenticidade destes princípios poderíamos pensar que todos os colaboradores numa organização estão sujeitos a algo semelhante do tipo, responsabilidade empresarial, para não dizer universal, visto que qualquer dos nossos actos poderia ter consequências boas ou desastrosas para a realidade em que estamos inseridos. Não será exactamente o cenário em questão mas a verdade é que pequenos actos ou omissões, por mais insignificantes que nos pareçam, podem originar acontecimentos desastrosos dentro de uma organização. Veja-se por exemplo um caso prático, já com alguns anos, e que aconteceu num hospital, que poderemos chamar de «Santa Piedade» (nome fictício), e no qual as consequências poderiam ter tido proporções mais graves. O impacto crítico da situação faz lembrar no limite um cenário que parece corresponder à lei básica da Teoria do Caos e ainda porque se afirma que a evolução deste sistema dinâmico depende crucialmente das suas condições iniciais (*tabela 1*).

⁹ Efeito Borboleta: Edward Norton Lorenz (May 23, 1917 - April 16, 2008) foi um matemático meteorologista Americano e que foi pioneiro no estudo da *Teoria do Caos* designado como o *efeito borboleta*.

Exemplo: Uma paragem de sistema no Hospital de «Santa Piedade»

O hospital de Santa Piedade possui mais de 1500 camas e cerca de 4 mil funcionários e 40 especialidades. É conhecido por alguma eficiência quando se trata de dar resposta ao atendimento administrativo dos utentes nas Consultas Externas e Emergência Médica. A equipa das TIC é composta por aproximadamente 20 elementos entre os quais excelentes profissionais com largos anos de experiência sejam a nível de base de dados, *networking*, *operações* e até hábeis em planos de contingência das TIC. O hospital não tem políticas de segurança implementadas mas do ponto de vista tecnológico têm implementados alguns mecanismos, tais como *anti-virus* global e uma *firewall*, que tendem a minimizar o impacto de eventuais ameaças. A equipa das TIC é responsável por gerir um centro de dados com algumas dezenas de servidores bem acomodados e um sistema central que gere a componente administrativa e financeira das actividades do hospital.

Situação: Um dia este hospital conheceu uma paragem total do sistema central que entupiu por 24 horas, toda a linha de atendimentos, de facturação, e tudo o que depende destes. Toda a equipa das TIC se dinamizou para resolver o problema verificando simplesmente que o servidor de alta disponibilidade estava desligado. Imediatamente se iniciou um processo de arranque do sistema operativo e carregamento das bases de dados, que já por si tem imensa complexidade, e depende do *know how* e disponibilidade de pelos menos duas entidades de *outsourcing*, para logo de seguida se verificar que este se recusava a iniciar porque simplesmente um outro recurso, disponível nas redes informáticas, lhe tinham absorvido a identificação.

Diagnóstico: O servidor de alta disponibilidade, como medida de protecção, foi concebido de raiz para desligar caso encontre no meio algum recurso a tentar tomar-lhe a identificação de rede. Enquanto o recurso, que tiver a sua identificação de rede, não for ou desligado ou libertado do meio não será possível voltar a “levantar” os servidores de alta disponibilidade, de uma forma totalmente operacional.

Ação: Descobrir e retirar do meio, o recurso que responde a um identificador de rede igual ao utilizado pelo servidor. Através de ferramentas de diagnóstico de redes procurar identificar o nome do recurso para que possa ser fisicamente localizado.

Relatório técnico: *A equipa dos serviços TIC verificou que o servidor central realizou um shutdown automático quando detectou, na rede informática, um equipamento que tinha o mesmo identificador de rede. Utilizando um comando de resolução de nomes detectamos que o recurso estava designado como «PCTrab_SecUnidade». Esta identificação para além de nos sugerir que se tratava de um posto de trabalho PC também indiciava que pudesse ser uma secretaria de Unidade. Existem mais do que 80 postos de trabalho, designadamente que possam ser de secretarias de unidade, localizados em qualquer um dos 40 serviços do hospital. Questionámos, mas sem resposta satisfatória, todos os serviços na procura de algum PC que recentemente tivesse sido alterada alguma configuração de rede. Percorremos então todos os*

Tabela 1: Cenário real adaptado ocorrido num hospital em 2001

É possível verificar que o impacto deste acontecimento, que poderia ter tido implicações mais penosas, dependeu inteiramente das condições iniciais. Ou seja, o comportamento do sistema, mais propriamente a paragem e o *downtime*¹⁰ dependeu da sua situação "de início". Se analisássemos a situação sobre outra condição inicial, provavelmente ela assumiria outros resultados e mostrar-se-ia diferente da anterior.

¹⁰ *Downtime*: tempo de paragem de serviço

	Condição inicial	Impacto	Situação preventiva
1	<u>Identificação do Recurso:</u> Uma política ou regra a existir não foi utilizada ou compreendida pelo técnico.	Não é possível saber com precisão a localização física do recurso (Serviço, Ala ou Piso);	Deveria ter existido uma política, a ser seguida, de identificação dos recursos em função das tarefas, serviços e localização física;
2	<u>Deslocação do Recurso:</u> Uma política ou regra a existir não foi utilizada ou compreendida pelo funcionário.	Não é possível localizar fisicamente o Recurso (Serviço, Ala ou Piso);	Deveria ter existido uma política, a ser seguida, orientada à utilização dos recursos informáticos com penalidades para quem não cumpra
3	<u>Registo de movimentos:</u> Não existem registos de deslocação do referido imobilizado	Não é possível localizar fisicamente o recurso (Serviço, Ala ou Piso);	Deveria ter existido uma política, e procedimento a ser seguido, orientada aos registos de movimentos e actualizações do imobilizado
4	<u>Manipulação deficitária do sistema de movimento de imobilizado:</u> O registo de movimentos do imobilizado está muito desactualizado.	Não era possível detectar qual o número de postos que foram retirados ou instalados recentemente nos secretariados ou salas de reuniões	Deveria haver uma sensibilização e compromisso na utilização dos sistemas de registo e manipulação do inventário
5	<u>Falta de segregação de funções dos recursos e alta disponibilidade:</u> Não existe sistema de alta disponibilidade. Vários serviços de core dependentes de um único servidor físico.	Impacto da paragem do sistema é elevado	Deveria existir um sistema de alta disponibilidade real que assegura-se a paragem de um servidor com a reposição de outro e a segregação de vários servidores por funções distintas
6	<u>Não existia nenhum sistema activo de LDAP:</u> A validação obrigatória por utilizador não existe ou não está configurada no recurso	Permitiu o acesso indiscriminado ao sistema operativo, dados e configurações do recurso	É obrigatório que exista um servidor central de validação de utilizadores com privilégios de acesso por perfil. É obrigatório que na instalação dos postos de trabalho estejam configurados os recursos para esse fim.
7	<u>O utilizador tem acesso ao recurso com privilégios de administração:</u> Para além do utilizador ter entrado como anónimo teve privilégios de administrador do recurso	O utilizador pode alterar a identificação de rede do recurso	Devem existir políticas para garantir que não existem perfis generalizados e muito menos partilhados entre utilizadores
8	<u>Não existe nenhum sistema de monitorização de rede:</u> Não é possível fazer a monitorização e gestão dos recursos de rede	Não é possível detectar o <i>switch</i> no qual o recurso esta ligado	Deve ser garantido servidores e soluções de monitorização de redes (ex. servidor de RADIUS) ou típicos do fabricante que permita a monitorização de rede, de <i>switchs layer 3</i> a fazer <i>routing</i> que permitam à equipa técnica detectar qual o <i>switch</i> no qual os recursos estão ligados.
9	<u>Não existe contrato de manutenção reactiva para o sistema central de gestão administrativa e financeira:</u>	Pode afectar o <i>downtime</i> do sistema caso a equipa local necessite de intervenção externa por não conseguir responder seja a falha de <i>hardware</i> ou a qualquer outra competência que possa não ter.	O hospital deveria possuir um contrato de manutenção preventiva e curativa com tempo de resposta útil definido em função da criticidade da paragem do sistema.

Tabela 2: Cenário de condições iniciais

Provavelmente por falta de política ou sensibilização na manipulação de recursos informáticos o funcionário, suspeitando que ninguém há anos utilizaria o computador pessoal, “esquecido” junto a um secretariado, o tenha deslocado para junto do seu posto de trabalho. Tendo em conta as condições iniciais da *tabela2* e o facto dos serviços responsáveis pela gestão e imobilizado do equipamento não terem sido informados, foi penalizador.

As iniciativas de planeamento, implementação e gestão das TI são normalmente tidas de “vista curta” onde é normal procurar-se o caminho mais fácil até porque parece ser sempre o mais adequado e menos dispendioso. São inúmeros os projectos e arquitecturas mal concebidas porque do ponto de vista da gestão das TI não existiu uma preocupação clara em gerir, medir e controlar. Os objectivos normalmente são atingidos mas resumem-se a uma estratégia de resolução de problemas de forma imediata sem medir o impacto que algumas medidas podem causar. Procura-se satisfazer as necessidades ou solicitações de um utilizador ou grupo numa cultura de procura da satisfação imediata sem ter em conta por exemplo critérios que salvaguardam a segurança de perímetro e que podem exteriorizar, a longo prazo, efeitos de onda nocivos ou o «Efeito Borboleta».

1.2.3. Motivação Complementar

Uma outra fonte de motivação para a elaboração do estudo é poder aproveitar a oportunidade de juntar uma série de directrizes, provenientes de normas com nível elevado de maturidade e aceitação no mercado, e juntar conhecimento e experiência adquirida ao longo de vários anos no sector para assim disponibilizar uma *framework* de gestão de TI estruturado, a ser utilizado pelo gestor das TIC ou um executivo no apoio à gestão da actividade nas seguintes valências:

- Planeamento e controlo eficaz dos processos e dos recursos de TIC;
- Redução dos riscos inerentes à utilização da infra-estrutura de TIC;
- Análise de indicadores de benefícios resultantes de uma infra-estrutura segura.

1.3. Metodologia de investigação

A utilização de uma *framework* é uma ferramenta útil de estrutura na gestão das TIC. É necessário perceber qual ou quais os mais apropriados que cumpram os objectivos que se

pretendem. Se nos posicionarmos no controlo de processos de segurança podemos estabelecer, como ponto de partida, que a utilização de COBIT¹¹ para controlo e monitorização de processos de Governo das TI até ao ISO 20000¹² para a disponibilização de serviços e suporte até à ISO 27000¹³ para a Segurança, são boas abordagens utilizadas regularmente na indústria. No entanto o estudo é caracterizado por abordar estas e outras regulações de uma forma superficial e simplificada com o intuito de desmistificar um pouco o falso desalinhamento e sobreposição que por vezes parece existir entre as normas a nível europeu (CEN¹⁴), internacional (ISO) e outras.

¹¹ COBIT: *The Control Objectives for Information and related Technology* trata-se um conjunto de melhores práticas para a gestão das tecnologias da informação. Foi criado em 1996 pela Information Systems Audit and Control Association (ISACA), e o instituto IT Governance (ITGI).

¹² ISO/IEC 20000: É a primeira norma internacional para a gestão de serviços da TI. Foi desenvolvida em 2005 pela *British Standards Institute* e substituiu a antiga BS 15000.

¹³ ISO/IEC 27000: Faz parte de uma família de normas orientadas a um modelo de gestão "Information Security Management Systems (ISMS)". Vem incluído no grupo "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

¹⁴ CEN: the European Committee for Standardization

CAPÍTULO II

2. PRIVACIDADE & ACESSO À INFORMAÇÃO CLÍNICA

As considerações sobre segurança, que é relevante equacionar nas comunicações e na partilha de recursos de informação no âmbito dos serviços dos cuidados de saúde não são diferentes das consideradas em qualquer comunicação típica de outro sector de actividade, com possível excepção de que a identificação das pessoas envolvidas, no contexto da sua informação de saúde, é sensível. A informação de saúde é um bem importante e tal como qualquer outro tipo de informação de carácter reservado, o envio através de meios electrónicos deve ser realizado com a total garantia que a informação é entregue à pessoa certa, sem alterações e sem que ninguém entretanto a tenha conseguido ler. Estas características que são consideradas nos critérios de confidencialidade, autenticidade e integridade estão na génese da ciência que estuda a segurança da informação.

2.1. Contexto da Informação

2.1.1. Dimensões da informação

A Ciência da Informação tem estudado e investigado durante décadas não só as propriedades da informação mas também a sua identidade. Ou seja na procura da identidade da informação os investigadores terão levantado questões muito simples como por exemplo, “o que é informação?”. Muitos estudos tal com as dimensões da informação de *Jens-Erik Mai* [8], partem do princípio que a informação, quando transformada em conhecimento se trata da sua forma mais valiosa, contudo é importante que seja identificada e estruturada para que o recurso possa ser utilizado em função da sua natureza. A título de exemplo, se numa organização identificarmos que do ponto de vista cognitivo, um pensamento ou uma propriedade intelectual

de um funcionário é um recurso de informação valioso a ser preservado, então devem ser activados mecanismos para esse efeito. A informação deve ser protegida em função das suas características (pertinência, sensibilidade, natureza, etc.) e em função disso as medidas a adoptar devem ser diferentes.

Segundo *Jens-Erik Mai* [9] as 5 dimensões da informação são (*figura 1*):

Dimensão 1: Informação Abrangente:

Informação é tudo e tudo é informação. Desde os eventos, os espaços, livros e pensamentos. Informação são sinais e existe em todo o lado que circunde as actividades do homem permitindo a estes agirem, reagirem e cooperarem;

Dimensão 2: Informação num Domínio:

O contexto refere-se ao domínio no qual a Informação está situada e é utilizada. O domínio consiste nas pessoas, organizações, intenções, objectivos, etc;

Dimensão 3: Informação nas Organizações:

A Informação flui em todo o tipo de organizações. Seja de carácter formal como informal, é disponibilizada e utilizada em várias formas, tal como comprada, vendida, gerida, guardada, escondida, organizada e recuperada. As pessoas nas organizações controlam a Informação, agindo como gestores e partilham e utilizam-na para colaborar;

Dimensão 4: Informação nas Actividades:

Quando o homem interage transporta Informação. Ela está na base para todas as decisões. O homem utiliza a Informação no seu trabalho do dia-a-dia e nas actividades diárias;

Dimensão 5: Informação Cognitiva:

Pensar é Informação. Conhecimento é Informação. A Informação é a matéria-prima para a cognição. Quando as pessoas pensam, utilizam Informação. A Informação causa e permite às pessoas modificar a sua linha de pensamento.



Figura 1: Dimensões da informação. Adaptado de *Jens-Erik Mai*

2.1.2. Classificação da Informação

Para *Jens-Erik Mai* a Informação pode ser distinguida como fazendo parte de um processo de negócio ou de um recurso de informação ou até tecnologias [9].

- **Processo Negócio:** Colecção de peças de informação e bens tecnológicos que ajudam a suportar um processo de negócio;
- **Recurso informação:** Informação clínica, demográfica, actividade, financeira, investigação e desenvolvimento;
- **Recurso Tecnologia:** Servidores *web*, servidores de base de dados, *desktops*, dispositivos móveis, infra-estruturas de rede.

2.2. Contexto da Segurança

A Informação é um recurso que, como outros importantes recursos de negócio, tem valor para a organização e consequentemente necessita de ser devidamente protegida. Existe em diversas formas e formatos e pode ser impressa ou escrita em papel, guardada electronicamente,

transmitida por correio ou por meios electrónicos, apresentada em filme, ou transmitida por diálogos. Qualquer peça de informação pode ser perdida ou danificada através de inúmeras quebras de segurança. De acordo com Pfleeger [10], algumas das quebras da segurança surgem quando a Informação está exposta e sujeita a qualquer tipo de ameaça. Demasiada exposição pode sujeitar a revelação não autorizada de dados ou a modificação destes num ambiente sensível se, durante um ataque, forem encontradas vulnerabilidades - fraquezas encontradas num sistema de segurança e que podem ser exploradas.

2.2.1. A Segurança da Informação

Tal como outros recursos, a segurança da informação pode ser caracterizada por ter características únicas. O objectivo em promover a Segurança da Informação é para reforçar que se mantenham as características de máxima Confidencialidade, Integridade e Disponibilidade, qualquer que seja a forma e a pertinência que a informação possua e o meio na qual é partilhada [9] (*figura 2*).



Figura 2: dimensões da segurança da informação

Confidencialidade: Assegurar que a informação é acedida somente por quem está autorizado a aceder (*figura 3*).

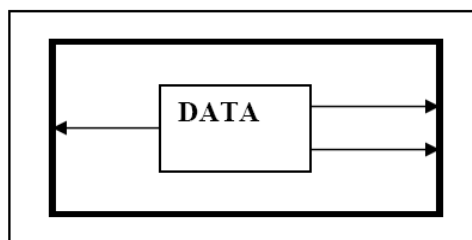


Figura 3: Confidencialidade dos dados

Integridade: Salvaguarda da veracidade e complementaridade da informação tal como dos métodos no qual deve ser processada (*figura 4*).

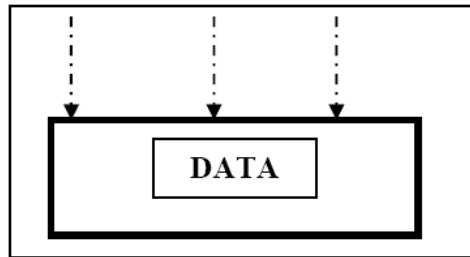


Figura 4: Integridade dos dados

Disponibilidade: Garantir que só devidamente autorizados, sempre que necessitam, têm acesso à informação e recursos associados (*figura 5*).

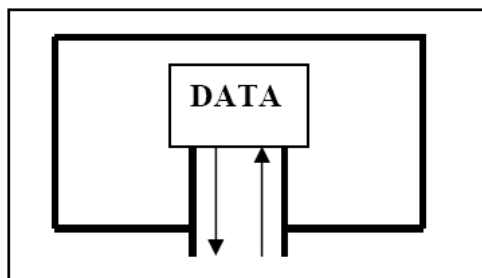


Figura 5: Disponibilidade dos dados

Existem outras propriedades da segurança que podem complementar as anteriores tais como a autenticidade, utilidade e posse que não substituem a confidencialidade, integridade e disponibilidade mas podem complementa-las [11]. Neste contexto também a ISO possui algumas normas que caracterizam a segurança da informação. Por exemplo a ISO7498/2¹⁵ no qual a definição da Segurança da Informação se identifica por ter cinco características principais:

¹⁵ ISO7498, parte 2 : Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture

identificação, autenticação, confidencialidade, integridade e não repudição. Para a ISO/IEC 27002 a definição de Segurança da Informação é a “preservação da confidencialidade, integridade e disponibilidade da informação através da implementação de um conjunto de controlos ajustados, que podem ser políticas, práticas, procedimentos ou até mesmo funções de software”. O caminho para a Segurança da Informação pode ser realizado através da implementação de um conjunto de controlos tais como as políticas, práticas, procedimentos, mudança nas estruturas organizacionais com a ajuda de funções de *software e hardware*. No entanto a forma de tratamento das actividades direccionadas à Segurança da Informação devem ser assumidas como actividades de gestão.

2.2.2. A Gestão da Segurança da Informação

A gestão da Segurança da Informação é uma actividade em crescimento em todas as áreas de negócio afectando a todos os níveis todas as posições na gestão das empresas desde o utilizador final até às administrações. Todos os funcionários numa organização deveriam compreender a importância da Segurança da Informação bem como que actos de negligência ou má conduta o podem penalizar. Para isso é importante que sejam conhecidos os riscos, ameaças e vulnerabilidades da organização quando sujeitas a ataques. De forma a gerir os riscos a gestão da Segurança da Informação dever ser proactiva no terreno, especialmente no inicio de desenvolvimento e/ou implementação de processos de negócio.

Quando uma organização está sensível em investir num modelo de segurança para proteger a sua informação, existe falta de informação estruturada sobre de que métodos dispõe e que métricas devem ser utilizadas. Normalmente, estas medidas podem ser adoptadas fazendo uso de *frameworks* com características de segurança. No entanto, com base nas respostas para as próximas para questões, e que se pretendem ver apuradas durante este estudo, será mais claro compreender os benefícios e estruturar os conceitos que estão subjacentes à utilização de modelos de gestão da segurança da informação.

- Quais serão as melhores práticas para implementar a Gestão da Segurança na minha organização?
- Qual é o melhor processo de avaliação dos riscos e como se pode/deve implementar?

- Quais as melhores práticas de protecção dos recursos de informação da empresa?
- Como podemos comparar os esforços de protecção da informação na organização com o melhor que a indústria tem para oferecer?
- Como se pode extrair visibilidade dos investimentos introduzidos na segurança e qual o retorno para a minha organização?

Estas e outras questões são esclarecidas nos próximos capítulos. É no entanto importante ter em conta que o estudo foi baseado nos pressupostos de que a gestão da segurança da informação é um problema de negócio e não de tecnologias e que a ISO/IEC 27001 é a única norma de certificação de gestão de Segurança da Informação para as organizações (*figura 6*).

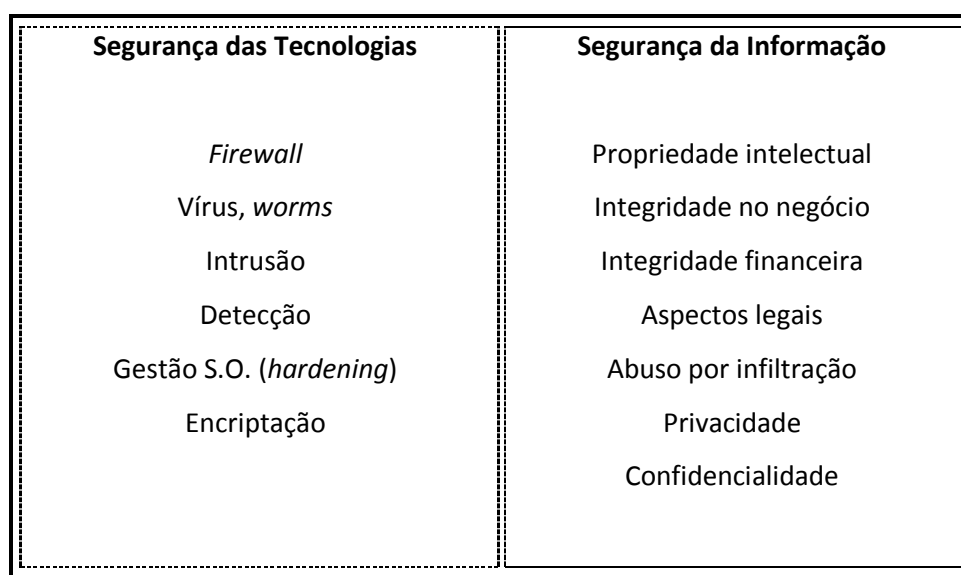


Figura 6: A Segurança da Informação como um problema de negócio

2.2.3. Segurança na Informação de Saúde

Proteger a privacidade da informação é o princípio básico a ter-se em conta para a troca de informação clínica. O controlo de acessos é normalmente considerado como o coração da segurança dos acessos aos computadores. O tipo de controlo de acesso mais utilizado na indústria e também na preservação da informação clínica é o acesso restrito ou controlado ao espaço físico e mediante credenciais com níveis de confiança aceitável, ou evidências de que por direito o utilizador pode ter acesso à informação. No que respeita à informação em formato electrónico um dos mecanismos mais utilizados para o controlo de acessos é o MAC -

Mandatory Access Control que obriga a que todos os profissionais, que tenham privilégios de acesso e manipulem informação de saúde, sigam um conjunto de regras, definidas numa ACL¹⁶, pelo gestor interno da informação clínica. O MAC permite um controlo dos recursos, e a que nível, podem ou devem ser acedidos por utilizadores ou processos [12]. O acesso à informação clínica seja em que formato esteja, deve seguir rigorosas regras estabelecidas e sobre um principal responsável pela gestão da informação clínica. No caso de um processo clínico electrónico o nível de acesso mais importante é o que regula o acesso a aplicações baseado nas funções dos utilizadores mediante um perfil [13]. Segundo um estudo do CINTESIS¹⁷ [14], foram realizados alguns testes de análise que comprovaram uma grande tendência para a partilha de credenciais de acesso entre os profissionais de saúde. Este estudo apresenta o conjunto de vulnerabilidades existentes através da má utilização das credenciais de acesso. Para assegurar a privacidade, o mínimo de controlos que devem ser implementados devem iniciar-se logo na concepção do recurso que vai permitir o acesso à informação (seja físico ou lógico) sempre baseados no conceito de *minimum need to know ou Access*¹⁸ e de preferência baseados num RBAC (*Role-Based Access Control*) que é análogo ao MAC, mas em vez de ter as permissões associadas aos níveis de segurança de cada utilizador, as permissões estão associadas às funções que desempenha.

2.3. Níveis de Maturidade da Informação Clínica e a Segurança

Segundo um estudo da *Irish League of Credit Unions*¹⁹ num relatório designado por *ICT Strategy 2007-2011* [15] de Abril de 2007 o nível de maturidade da informação clínica, no âmbito das TIC, está dividido em 6 níveis e no qual é explícito que em função do aumento do nível de maturidade na manipulação e tratamento dessa informação, aumento o risco e as vulnerabilidade. Normalmente os primeiros níveis (*figura 7*) de confiança são atingidos em muitos hospitais dos países mais industrializados. Os riscos nestas fases são moderados mas a partir do nível de maturidade 4, em que o PCE está mais focado no registo electrónico de práticas clínicas, o risco de exposição aumenta. O poder da computação permite acessos rápidos

¹⁶ Access Control Lists (ACL): Lista de acesso que armazena permissões e níveis de acesso a recursos de acordo com o perfil de utilizador ou de sistema.

¹⁷ CINTESIS: Núcleo de Investigação da Faculdade de Medicina do Porto.

¹⁸ Minimum need to know ou Access: Método básico de iniciar um processo afectando ao utilizador privilégios e conhecimento “zero” no momento do início do processo.

¹⁹ Irish Credit Union: is a group of people who save together and lend to each other at a fair and reasonable rate of interest. Credit unions offer members the chance to have control over their own finances by making their own savings work for them. <http://www.creditunion.ie/>.

à informação clínica tratada em tempo real aos clínicos permitindo cuidados mais efectivos na medicina baseada na evidência. No nível 5 já se espera que sejam aplicados mecanismos de segurança uma vez que existem elos de integração de outras especialidades com módulos específicos (por exemplo diabetes, doentes renais, risco cardiovascular, entre outros) que podem ser integrados na estrutura de *core* e partilhar a informação mais rica e disponível através da rede. No nível 6 em que estão subjacentes processos de melhoria contínua na procura de transitar todo o papel para meios totalmente electrónicos, incluindo componentes de multimédia, angiogramas, vídeos de endoscopia, RX digital e PACS, o risco está no máximo expoente e é necessário gerir os mecanismos de segurança adoptados.



Figura 7: Os 6 níveis de maturidade da informação clínica, adaptado *ICT Strategy 2007-2011*

2.4. Regulamentos

É importante que existam leis. E quando o que está em causa é o acesso e a manipulação de dados de saúde, a situação torna-se ainda mais sensível. Políticas de segurança e regular é o mínimo que se exige para protecção do ambiente técnico, físico e físico do seu fiel depositário. No âmbito do controlo de acessos não é suficiente a adopção de mecanismos sem que existe *a priori* uma política, com procedimentos de segurança, que abranja também quem faz a gestão dos utilizadores, para além de outras formas legais que orientem e responsabilizem os utilizadores pela forma descuidada com que podem vir a manipular os recursos. Manter a segurança da informação é suposto ser uma actividade diária .

Um sistema de informação em Portugal para estar certificado, no âmbito das linhas orientadoras que regulam a protecção dos dados pessoais deve ter o registo na Comissão Nacional de Protecção de Dados (CNPD)²⁰. Trata-se de uma Comissão Independente com poder e autoridade necessária que funciona em estreita colaboração com o Parlamento da Republica Portuguesa. Os seus principais objectivos são controlar e inspeccionar o processamento de dados pessoais em consonância com os direitos das pessoas, garantias e liberdades que pertencem à lei e Constituição Portuguesa. A nível europeu existe por exemplo outra entidade reguladora como a DPA (*Data Protection Act*)²¹ do Reino Unido que define uma base legal para a manipulação de informação dos dados pessoais. Embora o acto em si não signifique que haja obrigatoriamente privacidade, na prática implementa algumas medidas no qual o cidadão pode beneficiar e ter o controlo da sua informação de forma privada. Os organismos no Reunido Unido são legalmente obrigados a entrar em conformidade com o DPA sob o risco de severas penalizações.

²⁰ CNPD: Comissão Nacional de Protecção de Dados. É uma Comissão para o governo e protecção de dados pessoais.

²¹ DPA: Data Protection Act 1998: É um instrumento de legislação em Inglaterra para o governo e protecção de dados pessoais.

CAPÍTULO III

3. ESTRUTURA E GOVERNO DAS TI

Durante mais de uma década da era da informação que cada vez mais se tem verificado a necessidade de utilização da informação para a extracção de conhecimento que permita acções na decisão do negócio [16]. A informação é reconhecida, para algumas organizações, como um dos mais importantes bens estratégicos utilizados para a gestão. Os Sistemas de Informação e os serviços que lhe estão associados desempenham um papel indispensável para a persecução do negócio pelo que são recursos que necessitam de ser favorecidos de uma gestão apropriada. O conceito de governo relaciona-se geralmente com elementos originais da relação social, designadamente as regras, processos e os comportamentos através dos quais os interesses se articulam, os recursos são geridos e o poder é exercido no seio da sociedade.

3.1. Governo das TI

3.1.1. Governo empresarial (Corporate Governance)

Segundo a definição da OCDE (1999) [17] a governança ou governo empresarial (*Corporate Governance*) é o sistema pelo qual as organizações são dirigidas e controladas e está directamente relacionado com a capacidade de tomada de decisões e no qual assume um grande potencial de realização e uma constante verificação da performance das medidas correntes. O conceito é recente (finais do sec. XX e princípios do sec. XXI) e tem diversas definições embora o denominador comum esteja associado da necessidade de alinhamento entre gestores/auditores e *stakeholders*. Normalmente está relacionado com uma gestão consistente e com políticas organizadas. O facto de algumas organizações apostarem no governo é porque preferem projectos com processos controlados e alinhados com os objectivos

de negócio. E essa é uma das características que se lhes permite dar forma e terem personalidade suficiente para se protegerem do caos. A dependência dos negócios nas tecnologias de informação resulta no facto de que as matérias do governo empresarial já não podem ser resolvidas sem termos em consideração as TI e isso significa que o *Corporate Governance* deve conduzir e estabelecer um governo para as Tecnologias da Informação (*IT-Governance*).

3.1.2. Governo das TI (IT Governance)

De acordo com o dicionário de *Oxford*, o termo *Governance* é o acto de controlar, dirigir ou regular as acções de uma entidade, como uma empresa ou o estado, e portanto o *IT-Governance*, será o acto de regular os processos das TI [18]. Implementar um modelo de Governo de TI significa utilizar um conjunto de práticas e normas, delineados pela administração, técnicos e utilizadores de uma organização, com o propósito de garantir controlo efectivo de processos, melhorar a segurança, minimizar riscos, aumentar o desempenho, otimizar recursos, reduzir custos, sustentar as melhores decisões e em consequência esperar um alinhamento entre as TI com os negócios.

A 26 de Maio de 2008 foi lançada a norma internacional dedicada à gestão das TI (ISO 38500)²² (*figura 8*) que é baseada na norma australiana AS8015 de 2005²³. Esta norma é composta por três grandes áreas: Avaliar, Gerir e Monitorizar no qual se estabelece um guia baseado em seis princípios: 1) estabelecer responsabilidades, 2) planear as TI de suporte às organizações, 3) adquirir valor das TI, 4) assegurar desempenhos adequados das TI sempre e onde é necessário, 5) assegurar a conformidade formal das TI com as regras internas e externas e como 6) assegurar que o uso das TI respeita o factor humano. Estas áreas são a chave para as linhas de convergência que garantem que os nossos sistemas estão a trabalhar de forma conveniente, e no qual temos a capacidade de investir e aplicar sobre eles novas capacidades. Como podemos dar prioridade e gerir o desenvolvimento de aplicações, alocar capital para novas aquisições e saber quando está na altura de descartar dos sistemas legados. Estas são as questões que devem ser respondidas em qualquer programa de *IT-Governance*. Um projecto de Governo

²²ISO/IEC 38500, 2008: JTC 1 Information technology, Corporate governance of information technology

²³AS8015/2005: Australian Standard for Corporate Governance of Information and Communication Technology

efectivo pode ajudar uma organização a assegurar que os seus recursos de TI permanecem focados nas prioridades de modo que os compromissos com o nível de serviço são preenchidos e as decisões são tomadas com a informação necessária. Em resumo o *IT-Governance* para além de garantir ferramentas de suporte à gestão das TI também procura obter o alinhamento das TI com os objectivos estratégicos e financeiros da instituição. As TI por seu lado podem influenciar oportunidades estratégicas definidas pela empresa fornecendo informação vital para planos estratégicos. Deste modo o *IT-Governance* posiciona-se garantindo às organizações a capacidade em tirarem o máximo partido da informação.

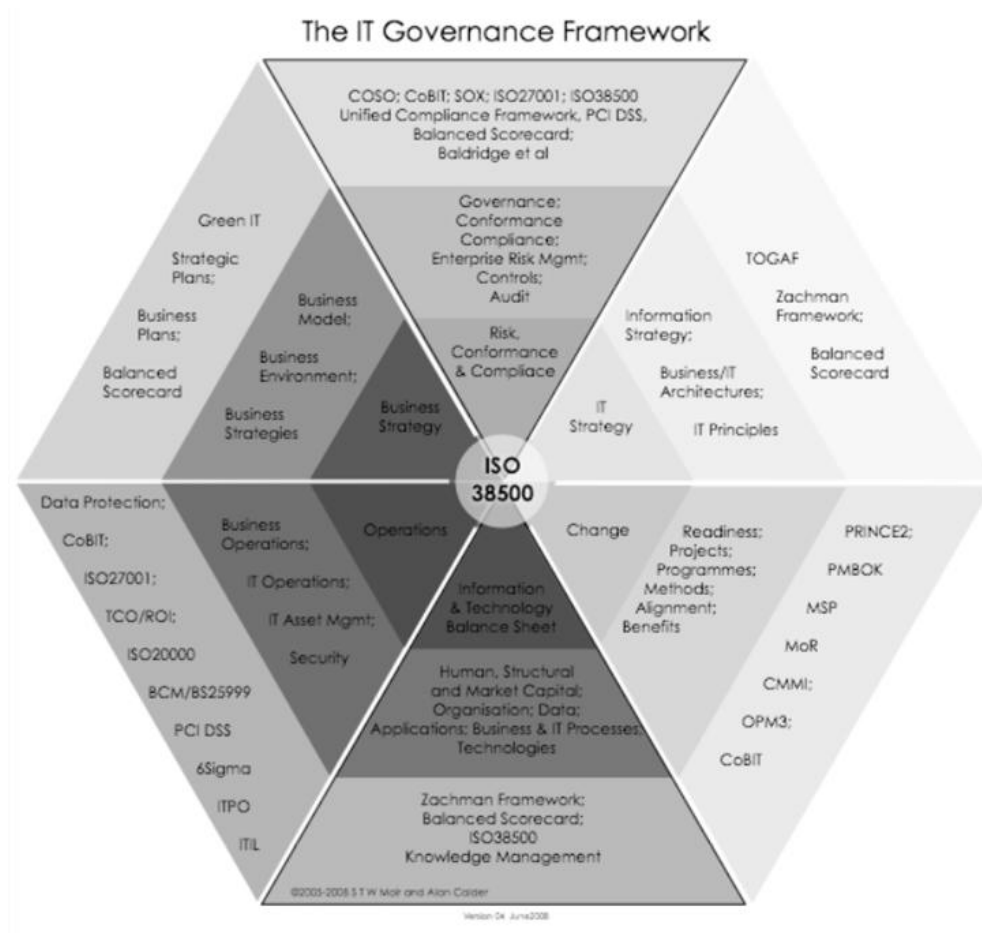


Figura 8: Framework IT-Governance 38500²⁴

²⁴ Framework de Calder-Moir, http://www.itgovernance.co.uk/calder_moir.aspx

3.1.3. Princípios do Governo das TI

Os 10 princípios do Governo das TI

Compilados pela *Harvard Business School* [19], segue uma versão adaptada dos 10 princípios para a boa governação da Tecnologias da Informação que dão orientações sobre o caminho a seguir para criar mais valor para as empresas.

1 – Desenhar activamente um modelo de governo: *O departamento das Tecnologias e dos Sistemas de Informação deve estar envolvido directamente com a estratégia da organização e os seus objectivos de desempenho. A estratégia de “tapar buracos” e resolver problemas pontuais limita o impacto estratégico das TI;*

2 – Procurar saber quando se deve reformular a estratégia. *Um modelo desenhado só é válido enquanto for eficiente não se exige definir tempos de duração, mas uma atenção particular à necessidade de um dia ter de remodelar a estratégia;*

3 – Envolver gestores seniores: *OS CIOs devem estar activamente envolvidos na gestão das TI para que a governação tenha sucesso, mas é necessário envolver gestores executivos de outras áreas nos comités para processos de aprovação de medidas;*

4 – Fazer escolhas. *Não é possível cumprir todos os objectivos e por isso devem ser identificados os que geram conflitos de execução e optar por aqueles que são estratégicos para o negócio da empresa;*

5 – Clarificar o processo de gestão de excepções: *Para acompanhar mudanças numa unidade de negócio é preciso saber abrir excepções em relação à arquitectura de TI e à infra-estrutura. Avaliar se estas fazem sentido e definir critérios para a sua aceitação;*

6 – Fornecer os incentivos certos: *Muitas vezes os sistemas de incentivos e recompensas não estão alinhados. É um problema que ultrapassa a governação de TI mas que também a afecta;*

7 – Definir responsabilidades na governação das TI: *Em última análise a administração é responsável por toda a governação, mas a delegação da responsabilidade individual ou de grupo normalmente recai no CIO, que assume o desenho, implementação e desempenho desta área. É preciso encontrar a pessoa certa mas não a separar do resto dos objectivos do negócio e*

garantir que esta crie uma equipa sustentável que apoie a implementação do projecto de governação.

8 – Implementar a governação aos vários níveis organizacionais: *Em grandes empresas, com vários níveis funcionais, é preciso considerar o governo de TI a vários níveis. Os pontos de partida são sempre os objectivos e estratégias globais, comuns às múltiplas empresas do mesmo grupo e diferentes geografias;*

9 – Assegurar transparência e formação: *Quanto mais transparente e mais conhecido for o processo de governação mais fácil é a sua implementação e o cumprimento das directivas por parte de toda a organização;*

10 – Implementar mecanismos comuns para as áreas fundamentais: *Vale a pena pensar de forma estruturada os recursos humanos, as relações com clientes e fornecedores, produtos, vendas, finanças e informação e as TI. A coordenação destes bens fundamentais da empresa parece óbvia mas nem sempre é implementada.*

A dependência que de momento os negócios têm das TI está implícito que não é possível resolver a implementação e controlo de medidas de *Corporate Governance* sem ter em linha de conta o governo das TI. Existem organizações a retirar partido de práticas de *IT- Governance*, normalmente impostas por coerção legal ou por iniciativas de motivação pessoal de algum gestor que acredita na fórmula que pratica. No entanto, logo que surtam resultados, espera-se que essas medidas sirvam para contribuir para uma mudança cultural mais profunda nas acções dos seus gestores. As empresas mais despertas já estarão a mover-se pela consciência de que isto reforça a sua credibilidade, segurança e solidez. Ao cumprirem os requisitos de conformidades, as organizações podem tomar melhores decisões, pois partem de informação com melhor qualidade, que permite melhorar os processos de negócio.

3.1.4. Gestão das TI (IT Management)

Ao conceito de *Governance* está subjacente na capacidade de se criarem mecanismos no qual outros possam vir a gerir eficazmente algum recurso, enquanto o *Management* é a actividade para se conseguir operacionalizar esses mecanismos. Para que o *IT-Governance* seja situado numa perspectiva prática é importante saber qual a orientação deste para o negócio e qual é o universo de relacionamento que este tem de ter com a componente de tecnologias. Denote-se

na *figura9*, onde é possível ver que na relação entre o *IT-Governance* e o *IT Management*, o *IT-Governance* é muito mais abrangente e concentra-se na *performance* e na transformação das TI para irem ao encontro no presente e no futuro das necessidades do negócio. Por outro lado o *IT Management* está focado na eficiência do fornecimento interno efectivo de serviços e produtos e na gestão das operações de TI para responder num curto prazo.

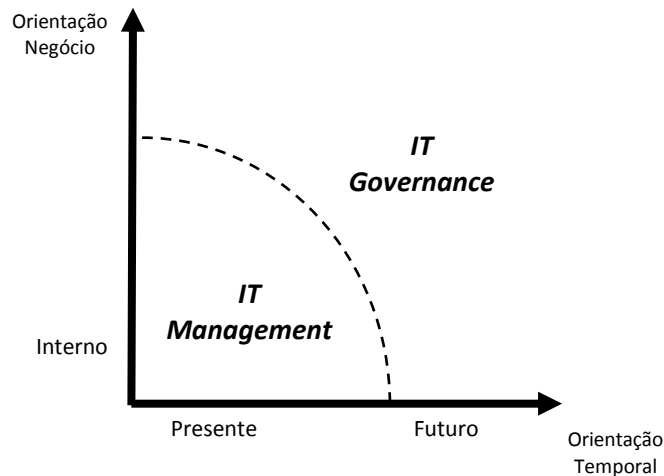


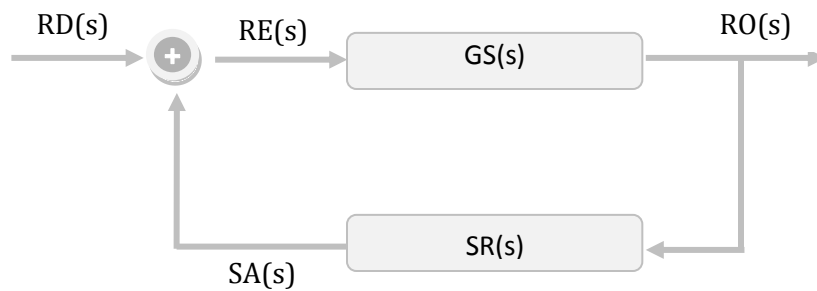
Figura 9: *IT-Governance* e Negócio, Adaptado a partir de modelo da ISACA²⁵

3.1.5. A Teoria do Controlo

A teoria do controlo é um ramo transversal à engenharia e à matemática que lida com o comportamento de sistemas dinâmicos. O *output* desejado é chamado de referência (*figura 10*). Sempre que ao longo do tempo um ou mais resultados necessitam de convergir para essa referência um controlador manipula os sinais de entrada para que se produza à saída do sistema o efeito desejado [20].

²⁵ ISACA: *Information Systems Audit and Control Association* . <http://www.isaca.org/>

Seja o exemplo seguinte com as respectivas funções:



$GS(s)$ = controlador

$RO(s)$ = referência obtida

$RD(s)$ = referência desejada

$RA(s)$ = referência actual

$RE(s)$ = referência errada

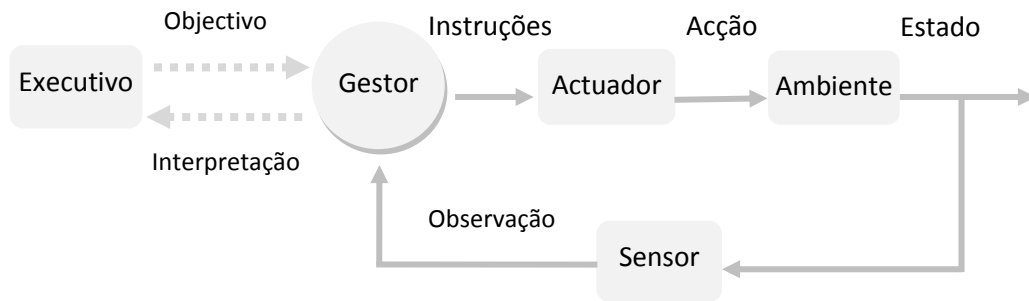
$SR(s)$ = sensor da referência

$$RO(S) = \frac{G(s)}{1 + G(s) \times SR(s)} \times RD(s)$$

Figura 10: Teoria de controlo moderno (modelo com compensação)

Onde se pode verificar que a saída do sistema, referência obtida (RO) depende claramente da função de leitura $SR(s)$ e da referência desejada.

Todos os processos seguem geralmente esse padrão básico de funcionamento seja uma válvula, a condução de um veículo (ex. *cruise control*) ou até a economia *per si*. O controlo de processos de *Governance* não foge a esta regra. Da mesma forma existem actuadores que exercem influência sobre o sistema; sensores que em tempo real monitorizam o estado e gestores cuja função é interpretar a informação proveniente dos sensores, compara-la com os objectivos (referência) e activar os actuadores no sentido de corrigir o seu estado para ir de encontro aos objectivos definidos pelo executivo (*figura 11*).



$$\text{Estado} = \frac{\text{Actuator}}{1 + \text{Actuator} \times \text{Sensor}} \times \text{objectivo}$$

Figura 11: Basic Control Loop²⁶

Se pensarmos numa organização no qual o **Executivo** é o *Chief Executive Officer* (CEO), um gestor sénior representa o **Gestor** e o sector de Vendas, Marketing, Desenvolvimento, etc. a agirem como **Actuadores** e a contabilidade como **Sensores**. Cada departamento da organização poderá ter uma estrutura similar orientada no sentido de alcançar determinados objectivos. Cada sistema de controlo possuiu um conjunto de leis, políticas e restrições que gerem a sua operação. Na Teoria do Controlo a este conjunto podemos designar por lei do controlo e que corresponde às políticas de governação de um determinado programa de *IT Governance* no qual o seu comportamento pode ser similar ao da *figura12*.

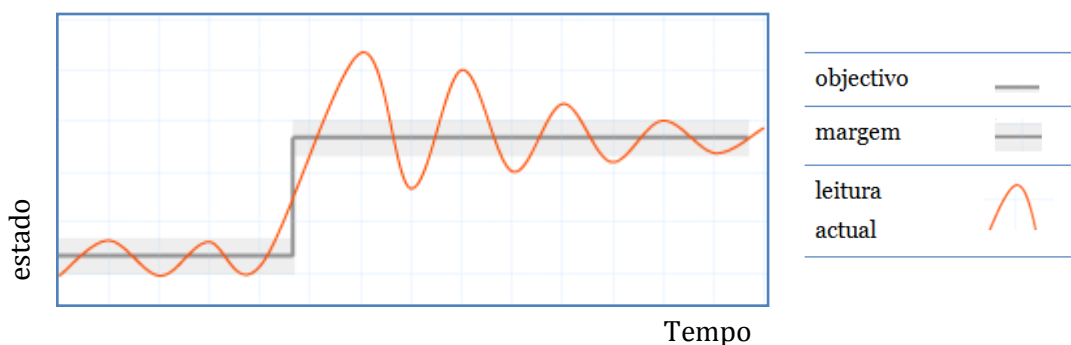


Figura 12: comportamento do controlo de um sistema ao longo de um tempo

²⁶ Basic Control Loop, Integration Consortium, DM Review Online, September 21, 2006

3.2. Governo nas organizações em geral

Segundo um inquérito da DTI²⁷ [21], 30% das organizações a nível mundial, não reconhecem que a informação relativa ao seu negócio pode conter características sensíveis ou críticas que lhes confirmem o estatuto de serem um bem de negócio. Segundo a norma ISO 38500 existem ciclos distintos de controlo que podem ser aplicados a qualquer infra-estrutura de tecnologias de informação de uma organização, baseado em *IT-Governance* para acções de definir e implementar processos, políticas e regras para o governo das actividades.

- **Projectos de desenvolvimento de aplicações:** Adicionam estrutura e disciplina à prática no desenvolvimento de aplicações. Controlo do código fonte, repositórios de dados, monitorização de tarefas, e planeamento de projectos e a gestão de software e a análise e as ferramentas de testes podem ser muito úteis para a implementação de projectos de *IT-Governance*.
- **Operação de sistemas em tempo real:** As aplicações de software para a monitorização das actividades de negócio podem ter neste cenário o papel de sensores. As aplicações de gestão das regras de negócio podem ter um papel importante para o gestor enquanto o software de segurança pode ser considerado como um actuador que protege os acessos de utilizadores não autorizados.
- **Gestão de portfolio:** Nesta componente é onde se decide desenvolver *versus* comprar; substituir *versus upgrade*, *in-house versus outsourcing*. São algumas das decisões consideradas como parte das gestão do portfolio das TI, e podem ser consideradas utilizando uma aplicação de gestão do portfolio de *bens* que providenciam informação sobre as dependências do suporte necessário e o impacto de custos. Um programa efectivo de *IT-Governance* pode ajudar uma organização a manter os seus recursos de TI focados nas prioridades, mantendo os compromissos com os níveis de serviços assegurados e decidir com base em informação precisa. É de crucial importância que os DSI das organizações conheçam na integra a arquitectura global do seu portfólio de aplicações de TI, conheçam os recursos de informação que se encontram disponíveis e em que condições e qual o papel que devem desempenhar para produzirem valor.

²⁷ DTI: Departamento de Comércio e Indústria Britânico.

Em resumo, o principal objectivo da aplicação do *IT-Governance* numa organização é:

1. Assegurar que os investimentos em TI geram valor de negócio e
2. Atenuar os riscos associados à introdução e investimentos das TI.

Pelo que estes objectivos podem ser alcançados se for implementada uma estrutura organizacional onde estejam bem definidas os papéis e as responsabilidades pela informação, os processos de negócio, aplicações e infra-estrutura (*figura 13*).

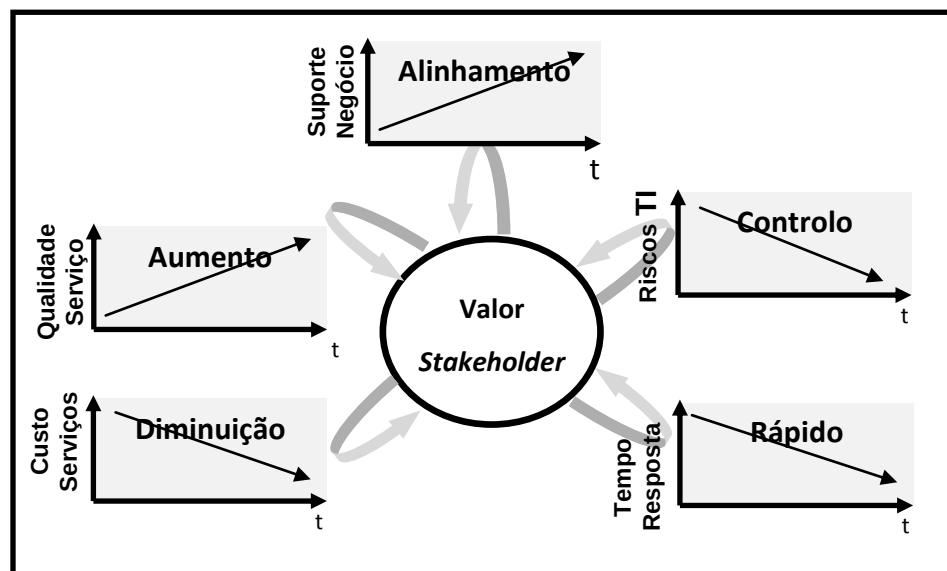


Figura 13: Benefícios expectáveis do *IT-Governance*

3.3. Governo nas organizações de saúde

Nos organismos de saúde, nomeadamente nos hospitais onde se encontre alguma maturidade que diga respeito à necessidade de gestão dos acessos aos recursos de informação, aguarda-se com ansiedade por orientações objectivas, proveniente de uma entidade de regulação, de como pode e deve ser gerido o seu conjunto de peças de informação em matéria de política que siga padrões de gestão do risco e da segurança de informação. A indefinição de regras e orientações e a falta de um repositório legal de documentação com as normas e conceitos mínimos que possam ser adoptados, na área das tecnologias informáticas e nas infra-estruturas de comunicação, redes e energia para que do ponto de vista funcional seja possível e acessível a pesquisa de informação que permita uma gestão operacional tais como por exemplo a implementação de directórios de utilizadores, servidores de comunicações, tecnologias *thin client*, *apoio ao utilizador* com qualidade de serviço, centros de dados energeticamente eficientes, entre outros. Porém não devemos menosprezar as arquitecturas de sistemas de informação, interoperabilidade, desenvolvimento, comunicação, arquivo, e até os mapeamentos das acções que manipulam informação de negócio.

No âmbito do Serviço de Saúde seria valioso que se promovessem:

- Um repositório central estruturado que concentre todas as regulações nacionais e internacionais com relevo para a Saúde, e o relevo que em Portugal deve ser dado;
- Um directório com vários actores ligados à gestão das TI onde pudessem ser acompanhados com a divulgação de trabalhos relacionados que estejam a decorrer nas instituições de saúde;
- A divulgação de trabalhos relacionados que estejam a decorrer na academia e no qual existe interesse em potencia-los como transferência da tecnologia;
- A criação de um espaço em que sejam propostos à academia novos estudos de avaliação, sistemas avançados, Apoio à Decisão e Investigação Operacional;
- Formação relacionada com a interoperabilidade, ITIL, DICOM, openEHR, entre outros.

3.4. A segurança das TI como habilitador de negócio

3.4.1. As exigências do mercado

A segurança não é um problema mas uma ferramenta que protege o nosso emprego e ajuda a impulsionar o negócio (Spafford²⁸, 2002) [22]. Uma aposta numa plataforma ágil e integrada para a segurança da informação pode garantir uma serie de oportunidades. Configure-se o exemplo na *figura 14* onde podemos constatar como quatro oportunidades se podem estender num determinado posicionamento. A oportunidade mais abrangente e a longo prazo é aquela que terá mais impacto para além do seu âmbito.



Figura 14: Oportunidades relacionadas com a gestão da segurança

Eficiência Operacional

O desafio para os gestores da segurança das TI é reduzir o custo total das operações em TI e em infra-estruturas e melhorar a produtividade de quem as utiliza. Do ponto de vista operacional uma plataforma integrada de segurança pode criar eficiência se:

- Centralizar a gestão das identidades dos utilizadores de modo que os ID e perfis dos utilizadores não tenham de ser criados e geridos em múltiplos sistemas;
- Centralizar toda a gestão de acessos de forma que a segurança não necessite de ser gerida em cada aplicação ou cada sistema operativo;

²⁸ Eugene Spafford: perito internacional da segurança - the executive director of Purdue University's Center for Education and Research in Information Assurance and Security (Cerias)

- Automatizar o acesso ou a inibição de todos os direitos de acesso das aplicações de cada utilizador de forma a eliminar que os administradores de sistemas tenham de dar/inibir acesso manual em cada sistema;
- Automatizar a gestão das vulnerabilidades de modo que os sistemas possam ser actualizados mais facilmente com actualizações de segurança;
- Permitir aos utilizadores que possam criar e gerir alguma da informação do seu perfil (por exemplo *passwords*) e evitar assim que isso tenha de ser realizado pelos administradores de sistemas ou pela equipa de suporte ao utilizador;
- Automatização e filtro de eventos na análise da gestão da segurança da informação. Permitir que os registos de actividade (*logs*) sejam agrupados e correlacionados de modo a ficarem mais visíveis os eventos mais importantes permitindo redução de tempo no esforço necessário pelos gestores da segurança, tal como a redução da probabilidade de ignorar as quebras de segurança.

Mitigação do Risco

Uma das oportunidades que a segurança da informação nos oferece é a capacidade de delimitar os riscos operacionais tal como as ameaças de *hackers*, *malware*, acesso não autorizados a recursos, tempo de latência até a desactivação de perfis de utilizadores que deixaram a organização, contas abandonadas, entre outras. São necessários planos para a delimitação dos riscos de modo a garantir que estes se encontram a um nível baixo aceitável. Estas ameaças não só têm impacto na criatividade da segurança dos bens da organização, como também tornam qualquer iniciativa de regulamentar e garantir a conformidade mais difícil. Existem duas áreas principais no qual uma efectiva gestão da segurança pode fazer beneficiar uma significativa delimitação do risco: a protecção de bens de forma a assegurar que os recursos valiosos da organização se mantêm seguros e acessíveis só a quem de direito; e a garantia da continuidade de Serviço de forma que os serviços disponibilizados a empregados, parceiros e clientes estão disponíveis quando necessários, sem degradação de qualidade ou nível de serviço. Uma solução integrada para a gestão das ameaças pode ajudar a assegurar a continuidade de serviços críticos de TI.

Conformidades e Auditoria

A gestão da segurança é o coração de muitas regulações das indústrias e dos governos, especialmente aqueles que lidam com requisitos relativos à privacidade de informação. Sem um infra-estrutura robusta de segurança que proteja sistemas, aplicações, dados e processos de acessos ou uso não autorizado, obter a conformidade é exigente. A chave para a conformidade com estas normas é garantir a implementação de um robusto conjunto de controlos de segurança. Esses controlos devem não só assegurar a validação e eficácia dos processos críticos de informação, mas também permitir que sejam facilmente auditáveis de modo a provar a *conformidade* a auditores internos e externos.

Habilitador de Negócio

Existe uma grande oportunidade relacionada com um sistema de segurança integrado no qual a aposta é em deixar entrar com segurança quem pretende fazer o bem permitindo o estabelecimento de iniciativas de negócio. Uma gestão efectiva da segurança permite que a infra-estrutura seja gerida de uma forma que mais facilmente faça crescer o negócio. Fortalece também a relação entre clientes e parceiros de uma forma que cria oportunidade de vendas de produtos e serviços adicionais seja com uma diversificação de serviços, melhoria do relacionamento com os clientes, melhorar a reputação, criação de um ecossistema robusto para partilha de aplicações e capacidade de reagir rapidamente à mudança das condições de mercado.

3.4.2. Desafios na implementação

Os gestores da segurança actualmente devem não só assegurar um ambiente seguro para proteger os bens da organização, como também a reputação da organização na indústria. Normalmente é obrigatório que estas actividades sejam implementadas a um custo mais baixo do que custos anteriores. Pelo que a pressão é que nas TI se faça cada vez mais com menos e isso provavelmente nunca mudará. Repare-se como algumas das áreas de intervenção levantam algumas questões importantes e que são uma pequena parte das áreas que devem ser endereçadas, e no qual os investimentos ainda podem ser consideráveis (*figura 15*).

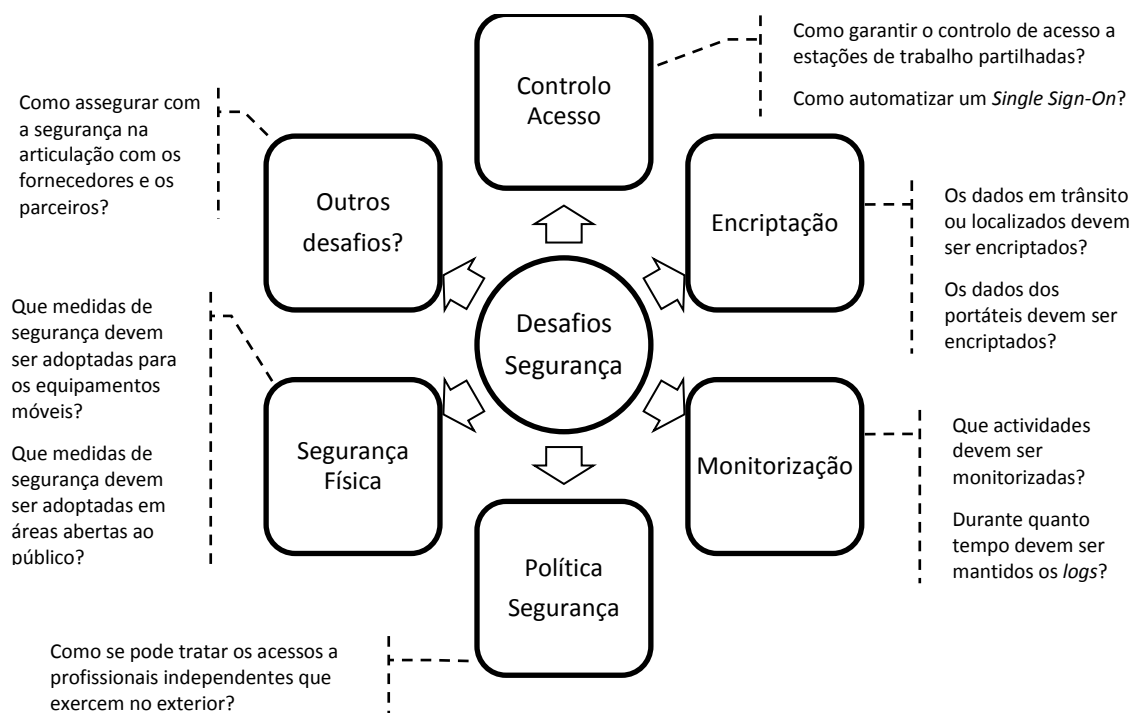


Figura 15: Exemplo de áreas a endereçar nas políticas da segurança

3.4.3. O lado iletrado do desafio

Um dos maiores problemas quando se enfrenta a necessidade de eleger um conjunto de acções com vista a endereçar medidas de segurança de uma forma generalizada numa organização é procurar compilar uma estrutura de competências e responsabilidades, delegando quem deve intervir, para fazer o quê e quando. É provável que não exista qualquer estrutura definida mas é peremptório que isso seja definido. Existe uma grande quantidade de dados espalhados pelas bases de dados e ficheiros das organizações e a falta de documentação, deixa prever que a informação esteja unicamente na “cabeça das pessoas”. Há dados vitais para o negócio espalhados entre computadores pessoais e da empresa, existe falta de segregação e responsabilização de funções, ausência de recursos dedicados a operações de segurança e também a falta de qualquer matéria-prima que permita auditar e recolher de evidências.

3.5. *Análise de Risco*

3.5.1. *Introdução*

Na linha da convergência das TI as organizações estão cada vez mais sujeitas a cenários potencialmente instáveis, quando se tem vindo a verificar o crescimento de um desvio entre a adopção das tecnologias e o controlo destas. Numa altura em que a informação é disponibilizada instantaneamente e em tempo real, identificar primeiro os riscos pode significar o sucesso ou insucesso de uma actividade. Uma vez que tem vindo a aumentar a dependência que as organizações têm nas tecnologias, o potencial impacto no caso de falhas de segurança é maior. Trata-se de um problema à escala global e que deve ser considerado não só pelas organizações privadas mas também por organismos públicos. Em consequência destas necessidades existem por exemplo implementações de *frameworks* de gestão como o Enterprise Risk Management da COSO (*Committee of Sponsoring Organizations of The Treadway Commission*), orientado para o *Corporate Governance*, e o Risk IT da COBIT (*Control Objectives for Information and Related Technology*), centrado no *IT Governance*. Nos EUA foi promulgada em 2002 a lei Sarbanes Oxley (SOX)²⁹ para promover a aplicabilidade de um conjunto de requisitos fundados em boas práticas e que obriga a que todas as empresas americanas e estrangeiras, com acções nas bolsas do EUA, cumpram esses requisitos. O SOX recomenda explicitamente o COSO para se efectuarem os controlos e a avaliação de riscos e o COBIT como instrumento de auditoria e avaliação das conformidades. Na Europa o equivalente para o controlo de riscos operacionais na indústria é o *International Financial Reporting Standards* (IFRS)³⁰ e o Basileia³¹ para a Banca. A nível internacional a ISO endereça as necessidades da gestão do risco coma norma ISO/IEC 31000:2009³², focada nos princípios e *frameworks* e a ISO/IEC 27005:2008³³ (antiga ISO/IEC 13335-2), mais focada nos processos de TI.

²⁹ SOX: *The Sarbanes-Oxley Act*. 2002 (SOX) é uma lei promulgada em resposta aos escândalos da Enron e da WorldCom financeira de forma a proteger os *shareholders* e o público em geral contra fraudes.

³⁰ IFRS: *International Financial Reporting Standards*. Normas e adoptadas pelo *International Accounting Standards Board* (IASB).

³¹ Basileia II: regula a determinação dos fundos destinados a prevenir os riscos de crédito, operacionais e de mercado.

³² ISO/IEC 31000: 2009 - "*Risk Management - principles and guidelines*".

³³ ISO/IEC 27005: 2008 - "*Information security risk management*".

3.5.2. Formas de reagir ao risco

O *IT Governance* é visto como um aliado nesta preocupação estratégica e identifica que os principais riscos que as infra-estruturas críticas estão sujeitas partem de *erro humano*, falha de sistemas e software malicioso. A questão a colocar para o problema do risco é como pode uma organização estabelecer um caminho para um programa de gestão de segurança da informação quando se reconhece que os riscos são reais e infinitos. O ambiente da informação é altamente dinâmico e os seus recursos são finitos. A implementação de uma solução terá sempre de incluir Pessoas, Processos e Tecnologias, e devem ser escolhidas uma das quatro formas de tratamento do risco (*figura 16*).

Transferir o risco Aquisição de seguros ou <i>outsourcing</i>	Evitar o risco Decidir não avançar ou não implementar
Aceitar o Risco Decidir que o nível de risco identificado está dentro do limiar de tolerância das capacidades da organização	Mitigar o risco Implementar controlos técnicos de mitigação de risco (por exemplo uma <i>firewall</i>)

Figura 16: opções para tratamento do risco

3.5.3. A avaliação e a gestão do risco

A gestão dos riscos não está unicamente orientada a identificar e a atenuar o potencial de possíveis ameaças. A gestão do risco pode sustentar vantagens estratégicas e diferenciais competitivos e novas oportunidades de negócio se estiver alinhada com outros objectivos de interesse. As organizações que apostam em iniciativas para a implementação de um projecto de gestão de risco antecipam também a sua visão sobre um *Corporate Governance*. Tomam essa iniciativa para agregar valor e alcançar oportunidades. Uma organização que possua maturidade

elevada na gestão da sua actividade terá certamente como sinal distinto a incorporação da prática de controlo dos riscos na sua cultura interna, identificando, gerindo e monitorizando os riscos (*figura 17*) de forma a mitiga-los e tornar mais robusta a segurança operacional.

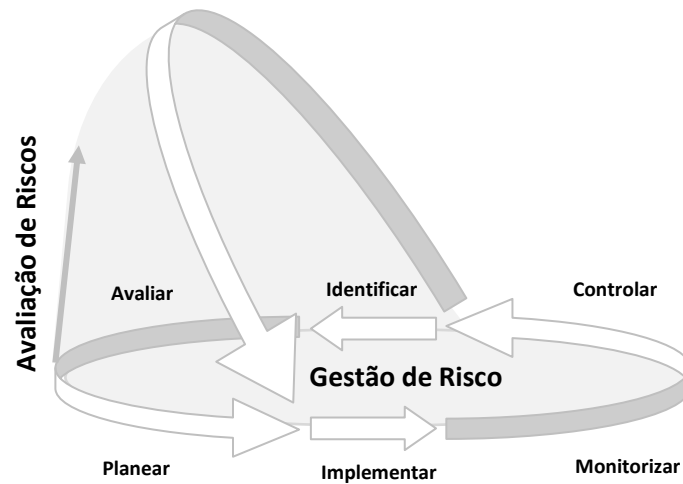


Figura 17: modelo de avaliação de riscos

CAPÍTULO IV

4. DEFINIÇÃO E EXPOSIÇÃO DO PROBLEMA

4.1. Exposição de contexto

Nos sectores da administração pública nomeadamente no sector da Saúde, por vezes existem decisões estratégicas, que são sustentadas em verdades incertas e que muitas vezes consumimos sem questionar. O acto de pensar e procurar saber parece que exige “muito” esforço. É muito mais fácil acreditar do que conhecer e mais confortável ainda é “comprar” o *know-how*. Este é o cenário mais provável de ser encontrado quando de uma forma generalizada não se encontra grande ansiedade nos gestores das TIC para a implementação de quaisquer mecanismos de segurança no acesso a dados críticos da organização. Tudo parece muito simples e porque se acredita que para garantir a segurança basta investir num bom *antivírus*, configurar bem uma *firewall* e monitorizar e controlar as partilhas de recursos. É necessário que as organizações, e nomeadamente a gestão da TIC acordem para a necessidade de utilizarem um código de prática que no mínimo ajude os gestores das TIC e executivos na influência de decisões estratégicas, que vise fundamentar por exemplo as iniciativas necessárias, mas pouco populares, e tornar a segurança uma das prioridades na organização. Tal como já referido no capítulo anterior, lidar com a segurança da informação é tudo menos um processo tecnológico. Está na altura de parar e planear o futuro pois este converge para a participação na implementação de uma norma acreditada e abrangente. Seja quais forem as medidas e até a norma o que é importante é assegurar a continuidade de processos de melhoria e a garantia de sobrevivência das medidas mesmo quando sujeitas a distintas políticas de gestão nomeadamente alterações do corpos da administração e dos directores de sistemas de informação. O conhecimento adquirido sobre os riscos relacionados com uma infra-estrutura de

TI pouco segura justificaria já acções de implementação de um sistema de gestão da segurança da informação (SGSI)³⁴ em qualquer organismo que manipule informação crítica. O princípio que está por detrás de um sistema de gestão, é que basicamente qualquer organismo que lide com informação sensível deve implementar e manter um conjunto de processos e sistemas para gerir os riscos a que os seus bens estão sujeitos.

4.2. Questões a problemas localizados

Para compreender a amplitude do problema é necessário conhecer minimamente as instituições de saúde, quais as políticas existentes para a segurança da informação, se é que existem, e qual o capital humano e investimento tecnológico que teria de ser afectado para as medidas a implementar. Em concordância, ao longo desta dissertação tentar-se-á dar resposta a um conjunto de questões direccionadas a justificar qualquer plano, investimento ou orientação para estas iniciativas.

Devem ser questionadas que padrões de medida poderão utilizar-se que justifiquem quaisquer iniciativas ou projecto de investimento num sistema de gestão da segurança da informação:

- **Organização:** *Quais os benefícios para o hospital quando alinhado com um sistema de gestão da segurança?*
- **Aspectos Legais:** *O que deve ser assegurado e como saber o que está ou não em conformidade?*
- **Operacional:** *A nível operacional o que pode ou deve ser realizado para a gestão de risco, gestão de incidências, etc?*
- **Negócio:** *Na Europa a legislação já convida os organismos públicos e privados a se posicionarem estrategicamente nas conformidades com as normas de gestão da segurança mas relativamente ao negócio da saúde onde está a mais-valia deste processo?*
- **Custos:** *Será um investimento demasiado alto e sem retorno?*
- **Humanos:** *É necessário envolver no processo de trabalho e formação todos os profissionais?*

³⁴ SGSI: *Information Security Management System* são um conjunto de políticas relacionadas com a gestão da segurança da informação, basicamente adoptada pela ISO/IEC 27001.

CAPÍTULO V

5. ARQUITECTURA EMPRESARIAL E SOCIAL

5.1. Modelo de Actuação

A ISO 27001 apresenta-se actualmente como a única norma para certificação na gestão da segurança da informação e a sua popularidade deve-se ao facto de que a sua abrangência a torna capaz de ser utilizada em qualquer indústria e a sua flexibilidade permite que possa complementar-se com outras normas de segurança para as TIC (*figura 18*).

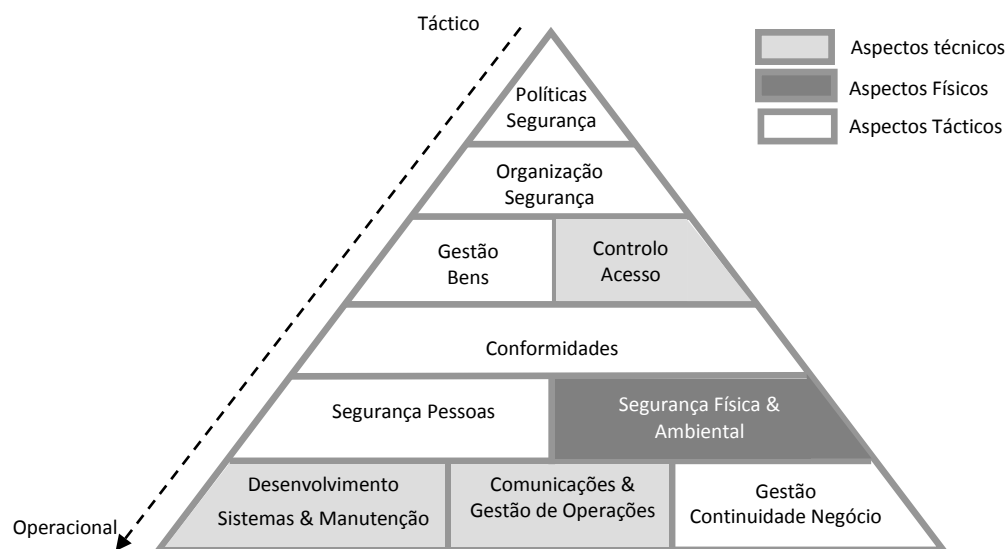


Figura 18: Cláusulas de segurança da ISO 27001

Desde os critérios mais táticos até aos operacionais a norma abrange todos os aspectos a ter em consideração e apresenta-se actualmente como a única norma para certificação na gestão da segurança da informação no qual tem uma abrangência a torna capaz de ser utilizada em qualquer indústria e a sua flexibilidade permite que possa complementar-se com outras normas de segurança para as TIC.

5.2. Do caos à estrutura

Os hospitais tais como as empresas estão numa constante mutação, pelo que é necessário um conhecimento profundo da organização, no qual é básico para que se possa definir e planear mudanças. Mudanças rápidas exigem melhor conhecimento da organização por parte da gestão. Nas organizações, embora o conhecimento individual seja suficiente para o tratamento de uma realidade mais próxima, não se trata de uma visão única da organização. É importante poder consolidar esses conhecimentos numa visão integrada que possua aspectos como por exemplo, as estratégias, as estruturas internas, os funcionários, competências e os seus objectivos tal como os processos e a informação de negócio, os sistemas e as tecnologias de informação. É comum ouvir falar-se em alinhamento das tecnologias e sistemas de informação com o negócio mas desconhecem-se propriedades ou métricas que possam expressar concretamente o que significa isso, e quando existe ou não o alinhamento. São necessários instrumentos e métodos para promover este alinhamento e por isso a Arquitectura Empresarial propõe-se precisamente a angariação deste conhecimento através da representação dos múltiplos aspectos que constituem as organizações, de forma a permitir práticas metódicas e continuadas de evidenciar e corrigir eventuais desalinhamentos. O modelo de *Zachman*³⁵ [23] procura enquadrar de uma forma simples todas as representações dos intervenientes no desenvolvimento, gestão, manutenção e utilização dos SI e TI da organização. O modelo foi lançado em meados de 80 mas tem vindo a evoluir ao longo do tempo³⁶ e encontra-se adaptado aos dias de hoje. A arquitectura assenta em duas ideias chave: na construção de um sistema complexo como é um SI de uma organização, são produzidas várias descrições que representam as diferentes

³⁵ John Zachman: O primeiro conceito de Arquitectura Empresarial foi apresentado por Zachman no qual fornece uma framework altamente estruturada para a definição de uma empresa. Consiste em classificar em duas dimensões numa matriz cruzada com seis questões direccionadas (What, Where, When, Why, Who and How) com 6 linhas de acordo com a respectiva transformação.

³⁶ Uma evolução da matriz de Zackman está disponível em <http://zachmaninternational.com/index.php/ea-articles/100-the-zachman-framework-evolution>.

perspectivas dos diferentes agentes, e o mesmo produto de SI pode, para diferentes propósitos, ser descrito de formas diferentes resultando em diferentes tipos de descrições. O primeiro contributo de *John Zachman* é o lembrar que se pretendemos que tal como uma empresa a construção de um determinado sistema não contribua para o caos é necessário que este seja planeado, concebido e concretizado de forma a ser ágil e flexível. Se não planearmos, concebermos e desenharmos com esse fim em vista, o sistema não terá essa potencialidade. O segundo contributo é a certeza de que não há forma de planejar, conceber e concretizar sem representar. Se não for possível representar os múltiplos aspectos que constituem as organizações ou um sistema, não podemos planejar e construir de forma a apresentar as características pretendidas. John Zachman criou em 1987, um instrumento conhecido por “*Zachman Framework for Enterprise Architecture*”, para a representação das organizações. A arquitectura de Zachman visou introduzir várias perspectivas diferentes em relação ao mesmo sistema, focado nas questões dos seis “W” a que cada um deve responder ao seu nível (*What, hoW, Where, Who, When e Why*), tornando as diferentes valências verdadeiramente complementares e integradas para a viabilização do resultado global.

*“Só a existência de uma arquitectura pode responder às questões da **complexidade** e da mudança. É a única forma que a Humanidade tem de lidar com elas. Ao **caos** opõe-se a estrutura.”*

JOHN ZACHMAN

O objectivo é formalizar e disciplinar a representação dos sistemas de informação garantindo, a integração dos diversos componentes de informação da organização facilitando qualquer mudança ou transformação nomeadamente na implementação de modelos para a gestão da segurança da informação.

5.3. Lidar com a complexidade

5.3.1. A complexidade

Qualquer organização necessita de ser gerida baseada numa estratégia. Não interessa gerir de forma isolada unicamente os seus recursos. Para isso é crucial que os projectos de TI estejam estrategicamente alinhados com os objectivos de negócio. Muitas vezes o sucesso desses

projectos depende quase e exclusivamente das equipas escolhidas seja para a liderança como para a execução, e tendo em consideração a grande complexidade e multiplicidade de serviços disponíveis, considera-se premente uma distribuição eficiente dos recursos disponíveis e por vezes até a contratação de profissionais mais qualificados. A complexidade da saúde obriga à existência de uma arquitectura de sistemas e de profissionais altamente qualificados (Lapão, 2007) [24]. A palavra complexo é utilizada com alguma frequência e por vezes releva de explicações adicionais sobre de que assunto se trata. É normal expressões tipo: o problema ou a situação é complexa, ter uma solução para satisfazer esses requisitos é muito difícil. Deixa a sentimento de que a complexidade é o caos, ambiguidade, incerteza, confusão. Segundo *Edgar Morin* [25] curiosamente o significado é o oposto. A palavra complexidade vem de *plexus*, "partes entrelaçadas que se unem e formam harmonia". No aspecto social, seja pelos avanços tecnológicos, nível de maturidade das pessoas e pela diversidade de recursos que devem interagir, acreditar e agir numa perspectiva que o ambiente é de complexidade acrescida pode facilitar a introdução de medidas para formar harmonia e ajudar a perceber os comportamentos e resultados. Os hospitais normalmente são organizações complexas, seja pela falta de estrutura, pela diversidade de especialidades existentes, pelo volume de pessoas, cultura, e disparidade de tecnologias existentes.

5.3.2. O papel do CEO, CISO, CIO e CTO

Tanto para os executivos como para os gestores das TIC lidar com a multiplicidade de problemas que podem ser encontrados num hospital é um completo desafio e daí que implicitamente seja desejável que os profissionais sejam altamente qualificados (Lapão, 2007). É normal encontrar-se um CEO ³⁷ insatisfeito quando na mudança do mercado das TIC, inclusive políticas da saúde, a sua organização não consegue responder rapidamente. Esse cenário surge porque do ponto de vista de capacidade de resposta à mudança existem carências na capacidade de gestão de projectos, pouco investimento à mudança e provavelmente pouca autonomia do gestor das TIC. É tudo demasiado complexo e lento, milhares de linhas de código, plataformas diferentes, sistemas isolados e imensas dependências técnicas, humanas e financeiras. Por regra, nos hospitais em Portugal não parece que se encontram CIOs³⁸, que por definição teriam de ser directores de primeira linha responsáveis pela gestão da TIC, e que no mínimo assumissem um

³⁷ CEO – Chief Executive Officer. Presidente do Conselho de Administração de uma organização

³⁸ CIO – Chief Information Officer, Pessoa que assume as funções de direcção de um departamento ou unidade de sistemas de informação e que através de uma nomeação de assessoria ou participação no board da empresa.

cargo de assessoria ao conselho de administração com uma autonomia, que no âmbito do governo das TI, lhe permitisse fazer crescer a organização no tempo e no espaço.

Na adopção do conceito o líder das TIC, ou mais propriamente o CIO normalmente necessita que o CEO lhe proporcione respostas mais rápidas de forma a facilitar as decisões TIC, tornando tudo mais simples e lhe dê as condições necessárias para que este se possa multiplicar em diferentes funções e posturas que lhe permitam ser bem sucedido na implementação ou na alteração de estratégias. Para conseguir atingir objectivos e transformar a saúde o CIO pode ter que desempenhar funções de tecnólogo mas também de diplomata, estratega, professor ou até psicólogo.

CIO diplomata: o CIO deve ser cordial, paciente, moderado, firme e estar disposto a explicar e sensibilizar, para uma medida em que acredita, quantas vezes forem necessárias. Na perspectiva de implementação de medidas de optimização de processos, utilizando por exemplo arquitecturas baseadas em serviços, o CIO deve não só promover um projecto para a arquitectura do sistema mas também pensar em *IT Governance* promovendo entre outros modelos a participação de um comité de segurança para o planeamento de políticas de gestão da segurança da informação crítica. O governo é o que está antes de qualquer arquitectura de sistema e por isso é fundamental ter padrões e explorar todo o negócio do projecto;

CIO Psicólogo: o CIO deve ser capaz de quebrar resistências que existem à mudança, provando acreditar que o caminho traçado é o melhor e que todos os envolvidos vão ficar satisfeitos. Aceitar uma batalha diária de promover a harmonia e não deixar cair as expectativas que os envolvidos tenham;

CIO Estratega: o CIO que consegue convencer o CEO das suas capacidades de agilizar processos apresentando resultados práticos deixando de ser visto como alguém que necessita de ferramentas unicamente para distração ou protagonismo mas sim uma necessidade de negócio;

CIO Tecnólogo (CTO³⁹): O CIO que conhece com alguma profundidade os objectos, ambiente e desafios tecnológicos normalmente possui vantagens relacionadas com a capacidade de não ter

³⁹CTO – Chief Technology Officer

de se recorrer a consultoria especializada para serviços de infra-estrutura e oferece mais credibilidade aos seus clientes;

CIO Professor: não se pode estar à espera de uma nova geração de CEO que compreendam o valor das TI e como podem trazer vantagens competitivas. O CIO deve ser capaz de formar os CEO para a importância das TI promovendo conceitos e práticas de governação;

CIO Gestor da Segurança (CISO⁴⁰): o CIO deve promover um comité para a segurança da informação onde estejam incluídos um elemento da administração e um responsável pela segurança da informação. Este perfil, normalmente designado CISO (*Chief Information Security Officer*), deve ser capaz de entender a importância da segurança e agir com independência e autoridade de forma a responder a desafios tipo:

- Alinhar a segurança com a missão da organização;
- Ser capaz de interagir tanto com o nível executivo como o operacional;
- Ultrapassar a visão da segurança da informação para a gestão de riscos global;
- Estruturar e gerir a base de conhecimento operacional;
- Manter-se sempre actualizado em relação às novas ameaças, vulnerabilidades e tecnologias;
- Estar sempre actualizado em relação às novas normas e regulamentações da actividade.
- Gerir o crescente aumento da complexidade dos sistemas das TI;
- Atingir a conformidade segundo as regulamentações em vigor;
- Gerir a segurança com os melhores níveis de custo benefício.

5.3.3. Crescer no tempo e no espaço

Os projectos e as funções normalmente afectadas ao governo das TI decorrem de forma muito particular nas organizações uma vez que dependem da maturidade instalada em termos dos SI/TI, e da capacidade que o capital humano envolvido pode oferecer. Quer sejam os profissionais com carisma mais técnico, que asseguram funções para a resolução de problemas centrados nas tecnologias (*Chief Technology Officer*), ou por outro lado os especialistas com uma “terceira” capacidade, mais orientada à gestão (*Chief Information Officer*), e que têm mais facilidade em agir proactivamente e influenciar a transformação do negócio através de uma

⁴⁰ CISO – Chief Information Security Officer

adequada utilização dos SI/TI. Nestes casos supõe-se alinhamento constante das actividades com os níveis da gestão e do governo.

Na “distância” entre um CTO e um CIO (*figura 19*), embora na generalidade dos casos o exercício de competências destes profissionais se complementem, existem estádios de maturidade, em relação ao desempenho destes profissionais, e que podem ir desde a incerteza; cepticismo; aceitação; confiança até ao respeito, e que tendem a definir a credibilidade que o profissional terá junto das direcções, utilizadores comuns, e *stakeholders* em geral.

A gestão dos SI e das TI nas grandes organizações inicia-se normalmente, em boa prática, com funções segregadas, para as várias áreas de especialização. Num organismo onde normalmente não se vêem no curto prazo mudanças, é provável com frequência que reine a incerteza, cepticismo e em alguns casos um grande pessimismo face à capacidade que esse sector terá na indução de projectos de melhoria. Essas situações acontecem quando numa gestão puramente baseada nos SI/TI, e no qual se exigem alterações nas operações da cadeia de valor, os critérios de acção são exclusivamente operacionais e focados numa engenharia pouco mais que reactiva. O antídoto para ultrapassar e conquistar progressivamente fases mais maduras, seja de aceitação ou de confiança é progredir na maturidade da gestão dos SI/TI, focando-se mais em serviços estratégicos do que operacionais e assim chegar ao governo das TI. Em cada estágio existem formas de gestão e de estar diferenciadas que à medida que ganham maturidade vão permitir à organização, como um todo, potenciar valor ao negócio e por consequência merecer a aceitação e o reconhecimento de todos.

Este tipo de abordagem, com a dignificação da gestão das TI ao nível da gestão, sustentarão vantagens estratégicas e diferenças competitivas para além de novas oportunidades de negócio se houver alinhamento com outros objectivos de interesse. Uma organização que possua maturidade elevada na gestão das suas actividades de SI/TI terá certamente como sinal distinto e de primeira prioridade a incorporação de práticas de planeamento e controlo de custos mas também uma gestão de riscos na sua cultura interna que permita a protecção dos seus bens e a aposta em planos de continuidade de negócio de forma a assegurar que os serviços disponibilizados a empregados, parceiros e clientes estão disponíveis quando necessários, sem degradação de qualidade ou níveis de serviço.

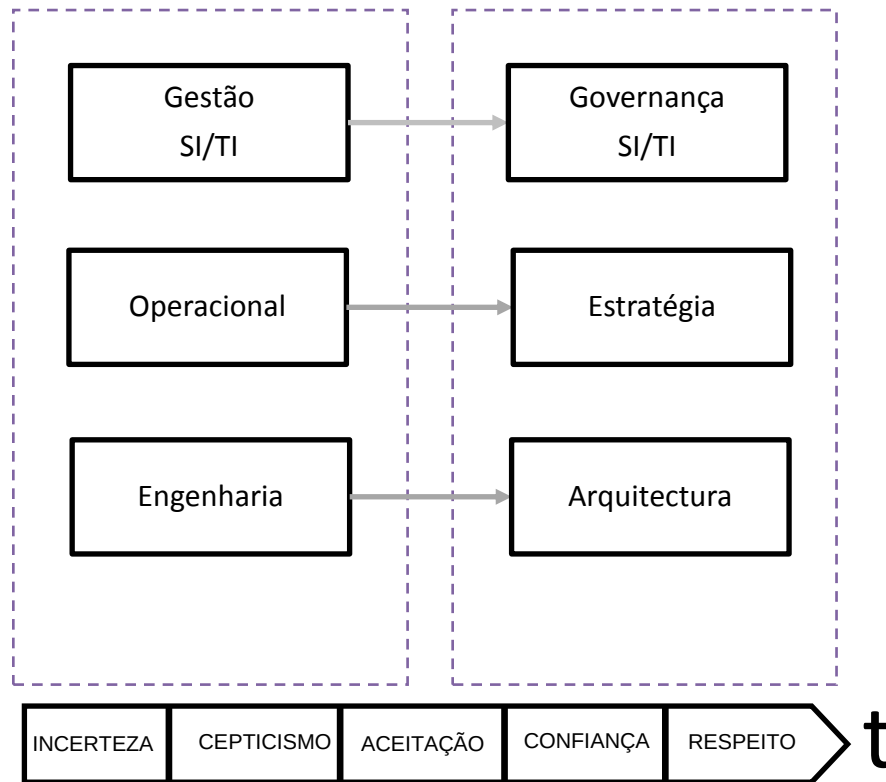


Figura 19: Os níveis de maturidade de um CIO

5.3.4. Competências nas TI e na Segurança

Em 2008 um inquérito (*figura 20*) encomendado pelo departamento inglês de negócios empresariais e reforma BERR (*Department of Business Enterprise and Regularoty Reform*), lançou um estudo em 2008 designado “*information security breaches survey*” [26] para a recolha, tratamento e análise de dados de uma amostra significativa de grandes e médias empresas do Reino Unido. Na auscultação, entre outros indicadores, apurou-se qual o nível de domínio, sensibilidade e qualificações formais em segurança que actualmente as equipas que lidam com as TIC nas empresas possuem. O estudo mostrou que dos responsáveis pela gestão da segurança da informação (quando existem), só 3% têm qualificações académicas ou certificadas em segurança, enquanto dos grupos responsáveis por gerir a segurança só 7% têm qualificações académicas ou certificadas na área. Um outro estudo de 2004 também levado a cabo no reino unido pela PWC, Microsoft, Symantec, Entrust e ClearSwift [27] já qualificava 22% desses mesmos profissionais com qualificações académicas ou certificadas em Tecnologias da Informação. Desde 2002 que não se vê grande interesse nas empresas em formar os seus quadros qualificados na segurança da informação, no entanto no mesmo inquérito da BERR demonstra que essas mesmas empresas estão cada vez mais preocupadas em gerir a segurança.

Desde 2004 até 2008 cresceram 13% das empresas que efectivamente implementaram as boas práticas ou a certificação ISO/IEC 27000. Das empresas inquiridas é comum o comentário de que é difícil encontrar no mercado pessoas qualificadas em competências de gestão da segurança. As pessoas devem ter mais do que capacidades técnicas e devem ter a capacidade de comunicar sobre questões técnicas com a gestão de uma forma que percebam. Seja dentro ou fora das empresas, pessoas com estas qualificações são escassas e muito válidas. Uma vez que os recursos internos não são qualificados significa que se deve ter recorrido de muito *outsourcing* e portanto implementar um modelo de segurança pode ser dispendioso.

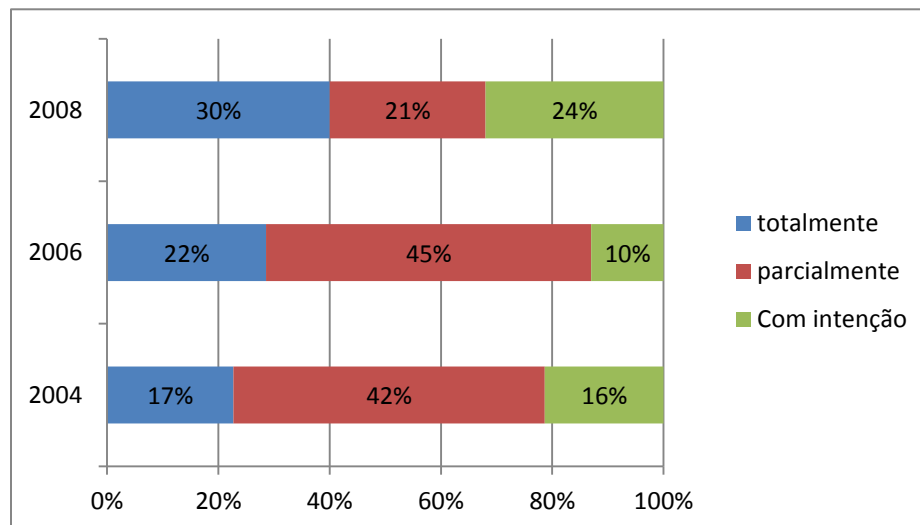
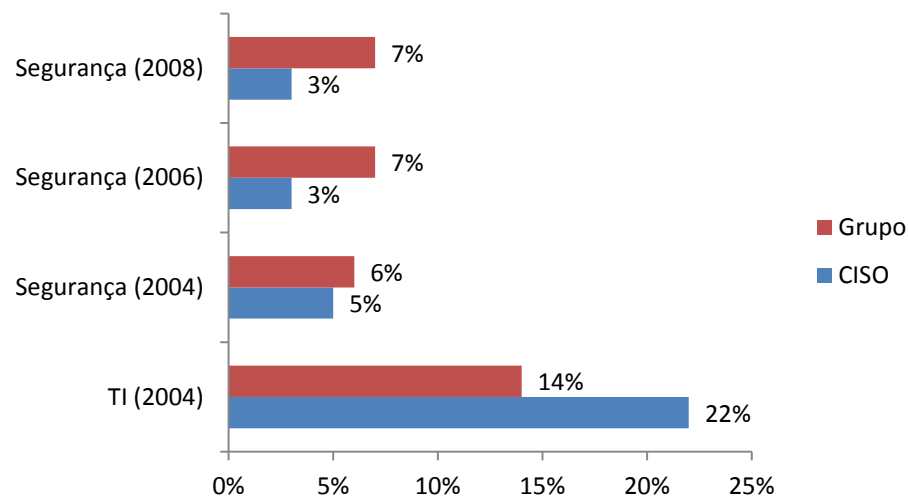


Figura 20: Inquérito às quebras de segurança “*Information security breaches survey 2006*” (PWC, Microsoft, Symantec, Entrust, ClearSwift)

Já em Portugal a situação ainda é mais *sui-generis* uma vez que o problema ainda está confinado à ausência de profissionais qualificados em TI na saúde, e por isso longe de ser ambicionado que se possam encontrar outras especializações em Governo de TI, gestão da saúde e gestão da segurança. Segundo um estudo produzido em Portugal pelo Instituto Nacional de Administração Pública (INA), ao cuidado do Prof. Luís Velez Lapão [24], demonstra-se que na saúde, nomeadamente nos hospitais, existe uma carência enorme não só de profissionais como de equipas qualificadas. Segundo o estudo os departamentos de Sistemas de informação (DSI) têm poucas pessoas, não têm qualificações académicas para as funções que desempenham, e muitos nunca tiveram formação específica de gestão nem das especificidades da saúde que lhes permitam elaborar uma estratégia que consiga lidar com a complexidade dos sistemas de saúde.

CAPÍTULO VI

6. INFRA-ESTRUTURAS E PROBLEMAS COMUNS DOS HOSPITAIS DO SNS

6.1. Metodologia de Investigação

Durante a última década tem sido possível perceber como tem vindo a crescer e a sustentar-se a introdução dos SI e TI nos hospitais públicos portugueses. Ainda que de forma empírica e com alguma margem de incerteza é possível estruturar uma relação que mostra a arquitectura que tem vindo a ser considerada seja para as infra-estruturas físicas como para as tecnológicas até ao desenvolvimento e à introdução de sistemas de informação dos hospitais. O método utilizado para esta investigação foi baseado na recolha de evidências, observações e aprendizagem adquirida na última década exercendo funções de gestão das tecnologias e da informação em organizações de saúde.

- **Evidências:** relatórios publicados pelos organismos centrais e regionais permitiram retirar uma imagem fiel do estado de maturidade em que se encontram os hospitais públicos em geral no que se relaciona aos sistemas e tecnologias da informação (políticas, deliberações, casos de estudo, etc.);
- **Observação:** A observação dos comportamentos das pessoas e dos sistemas durante anos de experiência e convivência com as comunidades;
- **Conhecimento:** Os casos de estudo nacionais e internacionais de entidades, empresas e da academia têm vindo a retratar também com algum rigor o estado de causa das TI e do nível de informatização dos hospitais em Portugal. Veja-se por exemplo relatório nacional da CNPD [28], que evidencia uma grande quantidade de desconformidades com a segurança dos dados ou outros estudos como por exemplo o apresentado por *Marc Holland da IDC Healthcare Insights* de 2008 [29] que referencia Portugal estando no nível de maturidade 1

que significa o nível mais básico de maturidade em sistemas de informação hospitalares (figura 21).

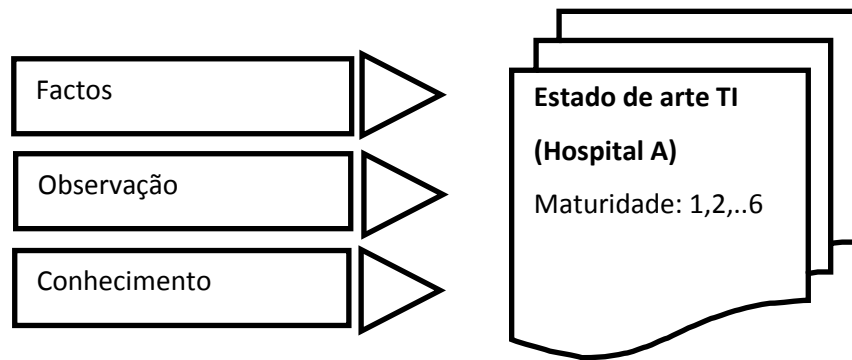


Figura 21: Níveis de Maturidade do Sistema de Informação Hospitalar

6.2. Modelo de camadas

Considere-se a arquitectura de SI/TI típica de um hospital público (figura 22). É comum assentar sobre uma infra-estrutura de rede, protegida ou não, com camadas de base de dados, aplicacionais e de interface com o utilizador. As camadas de ambientes aplicacionais, na sua concepção, normalmente dividem-se entre as soluções integradas e outras tantas mais isoladas, por vezes algumas são de sustentação de negócio e outras de suporte.

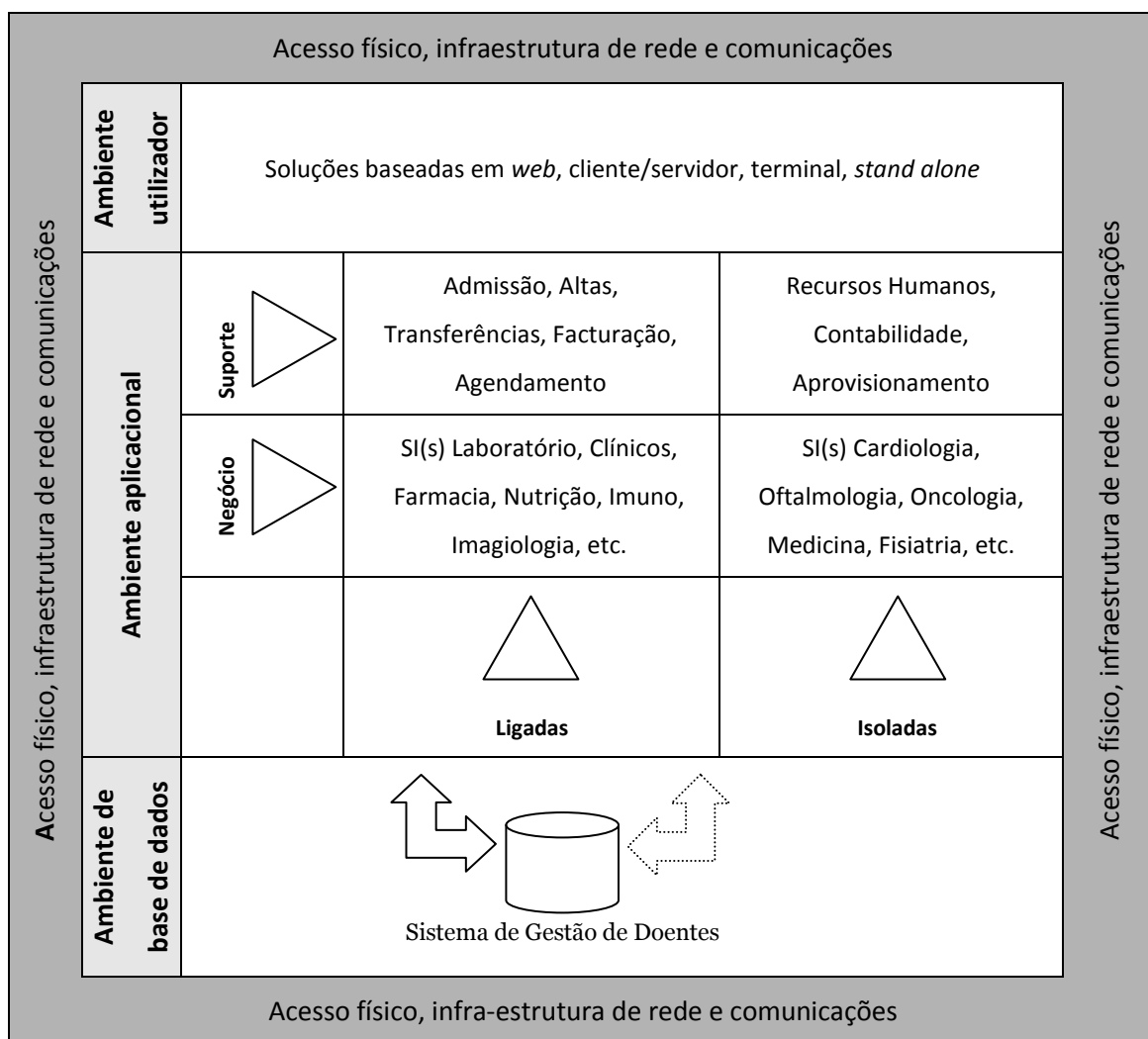


Figura 22: Exemplo da arquitectura típica de um ambiente de Informação Hospitalar do SNS

Para além de uma série de não conformidades e más práticas que é possível encontrar no *habitat* deste ou outro cenário similar, o que deveria ser necessário assegurar nos hospitais é uma separação lógica entre os dados administrativos e os dados de negócio de saúde, a fim de que os níveis de registo e os níveis de acesso sejam estabelecidos em função do tipo de informação tratada, qualidade e grau de confidencialidade dos dados.

6.3. Levantamento empírico de problemas mais comuns

Os problemas mais comuns nos hospitais podem ser do seguinte tipo:

1.	Existem poucas ou nenhuma políticas de segurança da informação e poucos estão familiarizados com normas como por exemplo, segurança, risco clínico e não clínico, ambiente, qualidade, etc.
2.	O número de profissionais da equipa de TI é reduzido e raramente existe uma aposta num gestor de segurança, coordenador ou comité onde exista a participação explícita de um elemento do Conselho de Administração.
3.	Existem diversos serviços de outsourcing mas falta a capacidade para a gestão de contratos e de serviços para um acompanhamento e monitorização da prestação de serviço dessas entidades (seja em presença física ou remota).
4.	Não estão definições grande parte das responsabilidades dos funcionários nas suas actividades dentro e fora do hospital.
5.	O serviço de recursos humanos não participa na gestão dos acessos e credenciais dos funcionários e não existe controlo no acesso à informação de gestão (<i>userid, password, biometria, impressão, cartão magnético, etc.</i>).
6.	Não existe documentação nem procedimentos para política de abertura de utilizadores no acesso à infra-estrutura, gestão de palavras passe, sistemas de <i>single sign-one</i> e gestão de identidades (bloqueio de acesso por cessação de contrato de trabalho por exemplo).
7.	Não estão definidos quais os recursos humanos com acesso à informação crítica nem quais os locais (zonas) críticas do hospital que deverão ter níveis de detecção e extinção de incêndios ou sistemas de controlo ambiental.
8.	Deveria existir uma monitorização do acesso de utilização de todos os recursos do hospital utilizados pelas entidades externas (nomeadamente bases de dados com dados do hospital, pastas partilhadas, serviços de rede, etc.).
9.	Deveria existir uma monitorização de sistemas com recurso a <i>logs</i> e auditoria com consola central para a gestão de eventos e alertas.
10.	Normalmente não estão descritas as políticas e procedimentos de <i>backups</i> .
11.	Não existe uma política documentada para a gestão da segurança das redes.
12.	Não são utilizados armários seguros ou cofres para salvaguardar informação crítica.
13.	Existem PCs portáteis em actividades de negócio, sem critérios de utilização, onde é permitida a utilização no exterior do hospital.
14.	A circulação interna da informação física não é efectuada de forma segura (processo clínico, prescrições, etc.).
15.	Existem acessos remoto a sistemas e aplicações pelos funcionários que não estão documentados nem registadas como incidências.
16.	Não existem registos de incidências ao serviço de <i>helpdesk</i> interno e gestão de stocks (conceitos ITIL para a gestão de TI) nem políticas de <i>harning (clear desk, clear screen)</i> .
17.	Não existem estudos para avaliação de catástrofe ou a implementação de planos e ensaios de continuidade de negócio e <i>disaster recovery</i> .
18.	Não existem políticas para a confidencialidade e privacidade em dados privados dos utentes.
19.	Não existem garantias de conformidades para com as legislações aplicáveis ao negócio.

CAPÍTULO VII

7. ELABORAÇÃO DE ESTRATÉGIAS PARA A RESOLUÇÃO DE PROBLEMAS

7.1. Disponibilizar e proteger a informação de saúde

As trocas de informação de saúde entre instituições e agentes estão muitas vezes sujeitas a incertezas relacionadas com a privacidade e o nível de segurança dessa informação. Os dados que são armazenados e trocados reflectem normalmente as condições de saúde dos pacientes, a informação financeira e os cuidados médicos que foram prestados. É previsível que essa informação só possa estar acessível a agentes autorizados mas ao mesmo tempo é fundamental que esses dados, especificamente quando se trata de prescrição de cuidados e terapêuticas não estejam corrompidos ou alterados seja por acidente ou de forma deliberada por terceiros. Verifique-se a pertinência da relação de risco (*figura 23*) quando comparada com os vários sectores de actividades.

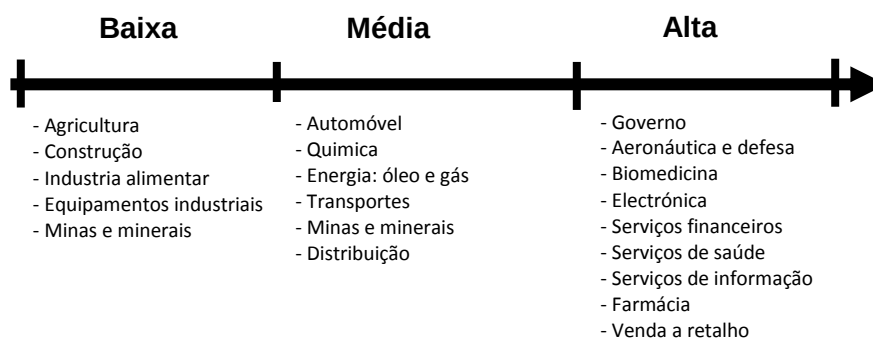


Figura 23: Nível de risco pela exposição de informação por sector de actividade⁴¹ [30]

⁴¹ Adaptado de CALLIO: Callio Technologies is the leading provider of information security compliance software and tools to help organizations of all types and sizes comply with internationally recognized standards and best practices.

A importância da segurança dos dados tem vindo especificamente a crescer desde a era da computação. A manipulação, perda ou a distribuição não autorizada de informação tem vindo a ser muito mais facilitada com os meios electrónicos do que na era do papel. De forma a assegurar a protecção total dos dados, muitas regulações e normas têm sido especificamente criadas para proteger informação desta natureza. Desde orientações técnicas e boas práticas até a questões de ética na troca de mensagens electrónicas.

7.2. Visão generalizada das normas

7.2.1. História

Pode dizer-se que o conceito moderno de normalização remonta aproximadamente a um século atrás quando vários países que se industrializavam sentiram a necessidade de definir regras para a utilização, em segurança, da electricidade. Assim, em 1906, constituiu-se em Londres a Comissão Electrotécnica Internacional (IEC)⁴², à qual Portugal aderiu em 1929, mantendo-se ainda como um dos 130 membros actuais. Mais tarde, no após a 2ª Guerra Mundial foi criada em 1947, uma nova organização com o objectivo de coordenar e unificar as normas internacionais, excluindo a área electrotécnica. A Organização Internacional de Normalização (ISO). No início da década de 70 surgem duas organizações europeias de normalização – o Comité Europeu de Normalização (CEN)⁴³ e o Comité Europeu de Normalização Electrotécnica (CENELEC)⁴⁴ – nas quais Portugal participou desde o início e ainda as integra. Finalmente, em 1989, é criado o Instituto Europeu de Normalização para as Telecomunicações (ETSI)⁴⁵ correspondendo ao desenvolvimento nessa área.

⁴² IEC - The International Electrotechnical Commission é uma instituição não governamental de standards internacionais sem fins lucrativos que prepara e publica standards internacionais relacionados com electrotecnia, electrónica e tecnologias relacionadas.

⁴³ CEN - Comité Europeu de Normalização, é uma organização sem fins lucrativos cuja missão é potenciar a implementação de um conjunto de standards e especificações na Europa de forma a potenciar o comércio global e o bem-estar dos cidadãos com base numa infra-estrutura comum de diálogo coerente

⁴⁴ CENELEC – Comité Europeu de Normalização Electrotécnica. O CENELEC é responsável pelas normas Europeias nos sectores da engenharia eléctrica.

⁴⁵ ETSI (telecommunication) – Comité Europeu de Normalização nas Telecomunicações. Em conjunto com o CEN e a CENELEC, o ETSI complementa os sistema de normalização europeia para a engenharia de telecomunicações.

7.2.2. Significado das normas

As normas são acordos documentados que estabelecem critérios importantes para produtos, serviços e processos garantindo que os produtos e serviços são adequados para os fins a que se destinam. O seu objectivo é estabelecer soluções por consenso das partes interessadas tornando-se numa ferramenta poderosa na comunicação entre agentes activos. Seja num contexto nacional, ou internacionais as normas promovem o desenvolvimento e anulam as barreiras à troca de informação, permitindo aos organismos claras vantagens num mercado global. A sua adopção providencia a identificação clara de referências que são reconhecidas internacionalmente encorajando uma competição justa e saudável nas economias de mercado livre. As normas facilitam a economia através do desenvolvimento de produtos com qualidade, confiança, grande interoperabilidade e compatibilidade, promovendo a facilidade na manutenção dos sistemas, e a redução de custos.

7.2.3. Importância da Normalização

O domínio da normalização estende-se a todas as actividades da sociedade. Seria impensável coexistir com um mundo onde cada país dispusesse dos seus próprios cartões bancários ou de telefone, rolos fotográficos, formato de papel, *dvds*, componentes dos diversos sistemas de transporte, entre tantos outros. Podemos assim concluir que, a inexistência de normas para tecnologias similares nos diferentes países, constituirá um entrave ao respectivo desenvolvimento, inclusivamente barreira técnica ao comércio, por contrariar a tendência de um mercado único não compartimentado. A nível industrial, o recurso ao espólio normativo, além de facilitar o comércio e a transferência de tecnologia, permite preços mais baixos para melhor desempenho e aumento de eficiência do produto, permitindo ainda aos consumidores terem uma maior confiança nos produtos e serviços que utilizam. Segundo a Comissão Europeia, a normalização estaria num ponto de viragem e defende que se está a aproximar o final do período de transição, no decurso do qual se passou de uma pequena estrutura de importância periférica para a situação actual de força crucial no desenvolvimento técnico.

7.2.4. Organismos de Normalização

O Organismo Nacional de Normalização (ONN) em Portugal e o Instituto Português da Qualidade (IPQ) definem as Normas portuguesas coordenando as actividades com outros organismos de normalização sectorial (ONS) reconhecidos, ficando com a responsabilidade a aprovação, disponibilização e homologação das Normas Portuguesas.

Os organismos Regionais (Europeus) de Normalização são o Comité Europeu de Normalização (CEN) e o Comité Europeu de Normalização Electrotécnica (CENELEC) e o Instituto Europeu de Normalização das Telecomunicações (ETSI).

Os organismos Internacionais de Normalização são a Organização Internacional de Normalização: Normas ISO e a Comissão Electrotécnica Internacional (CEI ou IEC).

7.2.5. Normas Portuguesas

As Normas Portuguesas (NP) são normalmente elaboradas por Comissões Técnicas de normalização (CT) no qual reúne um grupo de peritos da área temática, e é assegurada a possibilidade de participação de outras partes interessadas. Por definição, as Normas são voluntárias, a não ser que exista um diploma legal que as obrigue a um cumprimento obrigatório. Um dos principais órgãos técnicos coordenados pelos ONS são as Comissões Técnicas portuguesas de normalização (CT) que visam a elaboração de normas portuguesas e a emissão de pareceres normativos, em determinados domínios e, no qual participam, em regime de voluntariado, entidades interessadas nas matérias em causa, traduzindo, tanto quanto possível, uma representação equilibrada dos interesses socioeconómicos abrangidos. É portanto na defesa dos interesses da indústria nacional que se procuram interessar os fabricantes nacionais a cooperarem nas tarefas de normalização das CT.

Processo de normalização: este processo é constituído por várias etapas que passam pela votação pelos membros do comité de um projecto de norma, é produzido um esboço, é conseguido o consenso sobre o esboço que posteriormente é aprovado e publicado;

Processo de certificação: é um processo de verificação da conformidade com uma determinada norma. Contudo, os processos de certificação perderão todo o valor se a certificação não for efectuada por organizações imparciais e com competência reconhecida.

7.2.6. Normas europeias

No contexto europeu o CEN (*Comité Européen de Normalisation*) é uma organização privada sem fins lucrativos, fundada em 1961, que tem como missão promover a economia europeia no comércio global, o bem-estar dos cidadãos e ambiente assegurando uma infra-estrutura eficiente a todas as partes interessadas para o desenvolvimento, manutenção e distribuição de um conjunto de normas e especificações coerentes. É composta por 30 membros que trabalham em conjunto no desenvolvimento de normas europeias (ENs) em vários sectores para construir um mercado interno europeu de bens e serviços posicionando a Europa numa economia global. Mais do que 60000 peritos técnicos e grupos económicos, consumidores e outras organizações interessadas estão envolvidas nesta rede CEN num total de 460 milhões de pessoas. O CEN é oficialmente reconhecido como a entidade que representa o mercado de normas para sectores tais como a Electrotecnia (CENELEC) e as telecomunicações (ETSI).

7.2.7. Normas internacionais

A ISO (*International Standardization Organization*) cobre uma grande variedade de normas. Teve a sua origem em 1946 e é composta por uma rede de institutos nacionais de normas que inclui 157 países, com um participante por país, e um secretariado centralizado em Genebra na Suíça que coordena a rede. A ISO não é uma organização governamental embora ocupe uma posição especial entre os sectores públicos e privados de forma a servir de ponte e consensos entre as necessidades dos cidadãos e os requisitos de negócio sustentáveis para grupos de consumidores e utilizadores. A abrangência da ISO enquanto força de trabalho é composta por 2700 comités técnicos, subcomités e grupos de trabalho embora não cubra uma outra variedade de normas como as áreas de engenharia eléctrica e electrónica (IEC), telecomunicações (ITU) e das tecnologias da informação JTC1 (junção entre a ISO e o IEC), (figura 24).

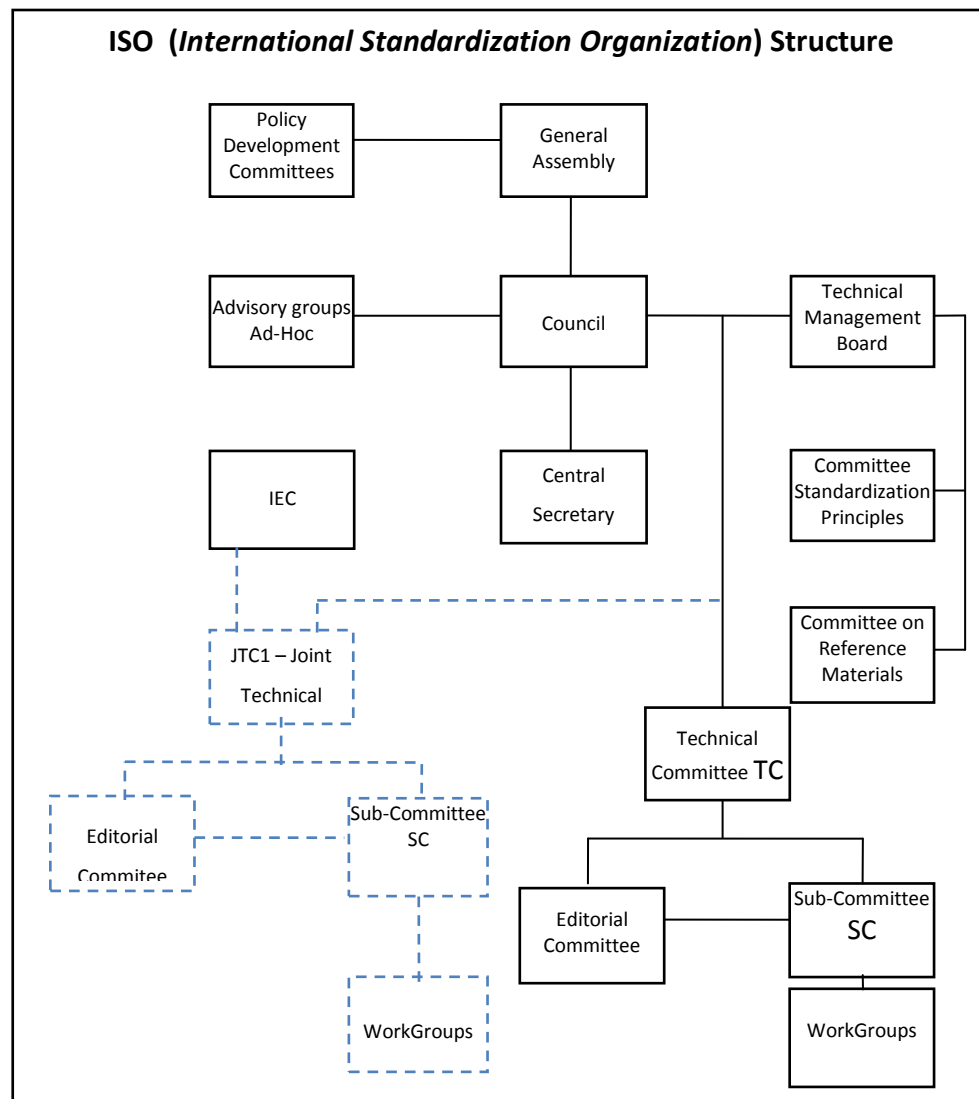


Figura 24: Estrutura da ISO (*International Standardization Organization*)

7.2.8. Normas para a saúde

O principal propósito dos serviços de saúde são providenciar serviços de qualidade aos pacientes e cidadãos não só confinados ao seu ambiente mas também em qualquer parte do mundo. As normas podem ser classificadas como padrões de mensagens, serviços, documentos estruturados, terminologias e protocolos de processos de trabalho e num contexto da saúde a utilização das normas são o pré-requisito necessário para o *eHealth Europe/CEN* nomeadamente:

- As comunicações de dados por exemplo permitem disponibilizar, de forma segura e abrangente, acessos on-line a bases de dados com por exemplo reacções adversas e suporte à decisão acautelando assim uma má administração de medicamentos evitando riscos de saúde e reduzindo custos;
- Permitir que os pacientes possam ter e dar acesso aos seus dados de saúde em qualquer ponto onde se encontrem;
- Melhorar a eficiência entre profissionais promovendo a utilização de ferramentas de colaboração capaz de utilizarem os sistemas de informação e de comunicação para apoio à prestação de cuidados.
- Potenciar a gestão e controlo da qualidade de dados agregados que possam estar disponíveis para os cidadãos e pacientes e possam ser utilizados seja por outras unidades prestadoras de cuidados partilhados como pelas autoridades públicas ou até unidades de investigação;
- Poder integrar-se módulos de diferentes fornecedores de produto através de normas de comunicações facilitando e atenuando o esforço de integração e normalizações pontuais que por vezes são necessárias realizar;
- Podendo reduzir custos por exemplo no esforço de integração que por vezes é necessário considerar com os diferentes fornecedores de soluções e que são um factor chave para a melhoria na agilização dos sistemas de prestação de cuidados de saúde;
- Poder expandir-se as comunicações de dados além fronteiras, principalmente numa Europa unificada e no qual o mercado dos sistemas de informação de saúde são praticamente Pan-Europeus e alguns já com projecção global.

Âmbito Europeu

No âmbito Europeu o CEN possui o comité técnico TC 251 que é um grupo de trabalho, que está focado na produção e regulamentação de normas na área dos sistemas de informação e das tecnologias de comunicação para a saúde. O principal objectivo é alcançar a compatibilidade e interoperabilidade entre sistemas e promover a modularidade e escalabilidade dos registos clínicos electrónicos. Os grupos de trabalho estabelecem requisitos para a definição de estrutura da informação de saúde de forma a apoiar os procedimentos clínicos e administrativos, métodos técnicos para o suporte à interoperabilidade entre sistemas. E adicionalmente são estabelecidos requisitos que dizem respeito à protecção, segurança e qualidade. O TC 251 é constituído por 4 grupos de trabalho:

CEN/TC251 Wg 1 - Modelos de informação: cujo objectivo é o desenvolvimento de normas europeias para facilitar a comunicação entre sistemas independentes;

CEN/TC251 Wg 2 - Terminologia: grupo responsável pela organização semântica da informação e do conhecimento de modo a ser utilizada de forma prática nos domínios da informática na saúde;

CEN/TC251 Wg 3 - Segurança e Qualidade: este grupo desenvolve em paralelo com as normas básicas da informática, prevenindo vulnerabilidades na quebra de confidencialidade e integridade da informação;

CEN/TC251 Wg 4- Tecnologia e interoperabilidade: grupo que promove normas que possibilitem a interoperabilidade de dispositivos e sistemas de informação em saúde tais como a inter-comunicação de dados entre dispositivos e sistemas de informação; a integração de dados com formato multimédia e a comunicação destes dados entre departamentos e outros utilizadores;

Entre outras normas e entidades a nível europeu e internacional o CEN/TC251 harmoniza com o Instituto Europeu dos Processos Clínicos Electrónicos (EuroREC)⁴⁶, o OpenEHR⁴⁷, o HL7, entre outros.

Ambito Internacional

No âmbito internacional o comité responsável por produzir normas para o sector da saúde é designado por ISO TC 215 e está dividido em 8 subgrupos (*Data Structure, Messaging and communications, Health Concept Representation, Security, Health Cards, Pharmacy and Medication, Devices, and Business requirements for Electronic Health Records*) (figura 25).

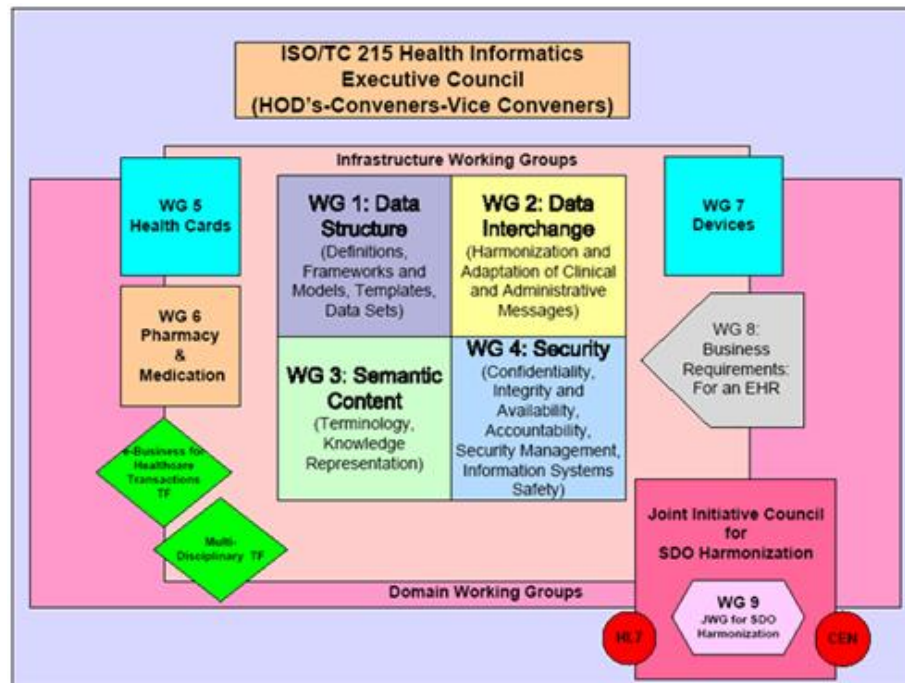


Figura 25:Estrutura da ISO/TC 215 Health Informatics

⁴⁶EuroRec: O Institute ou European Institute for Health Records é uma organização não governamental fundada em 2002 como parte de uma iniciativa PROREC. O Instituto está envolvido na promoção de serviços de qualidade prestados pelos sistemas de Registo Clínico Electrónico da União Europeia.

⁴⁷openEHR é uma norma aberta que descreve a forma de gestão, arquivo, acesso e troca de informação de saúde no âmbito dos registos clínicos electrónicos.

No sentido de enquadrar o conjunto de algumas terminologias existentes e a sua classificação funcional segue a *tabela 3*, no qual se pode evidenciar os comités europeus e internacionais e as nomenclaturas funcionais: M – Mensagens; S – Serviços; DE - Documentos Estruturados e T - Terminologias.

Sigla	Designação	Classificação Funcional
ASTM	<i>American Society for Testing and Materials - ISO</i>	DE
CEN TC 251	<i>European Committee for Standardization – Tec. Committee 251</i>	M,S,DE,T
ISO TC 215	<i>International Technical Committee - Health Informatics</i>	M, S, DE, T
DeCS	<i>Descritores em Ciências da Saúde</i>	T
DICOM	<i>Digital Image Communication in Medicine</i>	M, S, DE
HL7	<i>Health Level Seven</i>	M, S, DE, T
ICD/CID	<i>Código Internacional de Doenças</i>	T
LOINC	<i>Logical Observation Identifiers Names and Codes –</i>	T
MESH	<i>Medical Subject Headings</i>	T
NCPDP	<i>National Council for Prescription Drug Programs</i>	M
OMG	<i>CORBAMed Healthcare Domain Task Force</i>	S
RxNorm	<i>National Library of Medicine – Standards for clinical drugs</i>	T
SNOMED	<i>International medical Terminology</i>	T
UMLS	<i>Unified Medical Language System</i>	DE, T

Tabela 3: Classificação Funcional de Terminologias de Informática Médica

7.3. Estratégias para a resolução de problemas

Com a quantidade de normas e recomendações para a boa governação dos Sistemas e das Tecnologias para a saúde, é cada vez mais necessário estruturar essas áreas de conhecimento, de modo a tirar partido das *frameworks* existentes e utiliza-las como ferramentas úteis para potenciar a agilização dos processos de trabalho e aumentar a eficiência e eficácia nos organismos do SNS. Independentemente da origem geográfica das metodologias, normas e boas práticas, em Portugal e nomeadamente nos organismos do SNS existe a necessidade de compreensão, adaptação e enquadramento prático dessas *framework*. A maior parte das referências de governo que chegam a partir de diversas origens e focos, nasceram de estratégias de crescimento alinhadas pelo que em regra se complementam umas às outras.

Sejam algumas dessas áreas no qual assentam algumas metodologias para o governo das TI e o modo como estão posicionadas num organismo (*figura 26*).

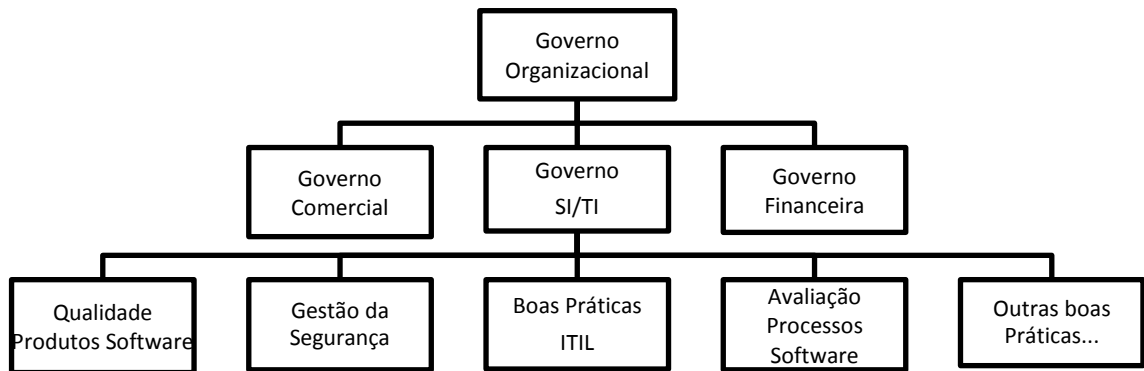


Figura 26: Estrutura típica de um governo para as TI numa organização

Ao governo das TI é comum encontrarem-se em textos de Alan Calder⁴⁸ associadas normas e boas práticas de Governo Organizacional tais como *Six Sigma*⁴⁹, *Balanced Scorecard*⁵⁰, TQM⁵¹, SOX, HIPAA⁵² entre outras, que obrigam as organizações a seleccionar e a implementar uma *framework* de controlo interno adequado que tratam das TI, para a gestão de processos proprietários, mas também para avaliação anual da eficácia utilizando o COBIT, o ITIL e a ISO 27002 (*figura 27*) (*tabela 4*).

⁴⁸ Alan Calder: Director fundador da organização IT-Governance Ltd. www.itgovernance.co.uk.

⁴⁹ Six Sigma: é um modelo para a gestão estratégica desenvolvido em 1981 pela Motorola. Foi actualizado em 2010 e procura ajudar as empresas a melhorar a qualidade e a eficiência dos processos de negócio com base na mitigação dos problemas identificados.

⁵⁰ Balanced scorecard (BSC): é uma ferramenta estratégica de gestão de performance que utiliza métodos e automatismos a serem utilizados pelos gestores no sentido de controlar as actividades da empresa e monitorizar ou prever as consequências dos resultados.

⁵¹ TQM: Total Quality Management (or TQM) é um conceito de gestão cujo objectivo é reduzir erros no fabrico de bens de indústria ou nos serviços, aumentando a satisfação do clientes em toda a cadeia de valor. Está normalmente associado ao desenvolvimento, exploração e manutenção de Sistemas na organização necessários ao processo de negócio.

⁵² HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 promulgado pelo congresso americano no sentido de proteger os seguros de saúde dos trabalhadores e familiares quando desempregados e no qual obrigou ao estabelecimento de normas nacionais para a transacção de informação electrónica de saúde entre as seguradoras, prestadores de cuidados e empregados.

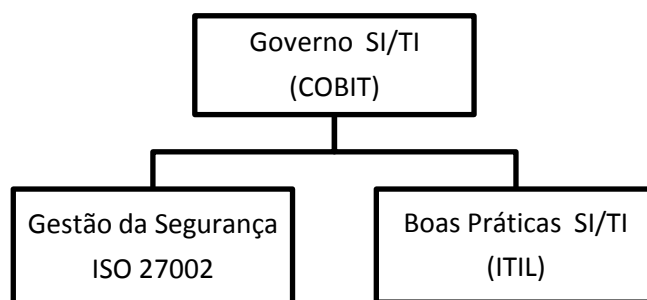


Figura 27 : Estrutura típica de um governo numa organização

<i>FrameWork</i>	<i>Descrição</i>	Benefícios
ITIL	Avalia os processos de gestão de serviços de TI da organização (com base em SLA ⁵³) e selecciona os processos prioritários a ter em consideração. Gera um plano de acção para melhoria dos processos das TI.	I.Utilização das melhores práticas II.Velocidade na análise III.Planeamento serviços IV.Visão executiva
COBIT	Avalia a estrutura das TI. Através da análise de conformidade e maturidade das TI com o COBIT dá-se prioridade às áreas de processo para o planeamento das actividades das TI.	I.Medir grau de maturidade processos de TI II.Visão da integração do negócio com as TI III.Identificação dos processos críticos das TI IV.Otimização dos investimentos em TI
ISO 27002 antigo (ISO 17799)	Avalia a estratégia e a estrutura da segurança da informação da organização conforme a norma ISO/IEC 17799 e prepara um plano de acção para eliminação dos pontos críticos.	I.Visão da segurança da informação na organização e integração com o negócio II.Planeamento das acções de melhoria
ISO 27001	Análise de um âmbito com vias à certificação ISO 27001. Inventário dos processos de negócio, sistemas e serviços e infra-estrutura de TI. Avaliação dos requisitos da norma. Apresenta um plano de acção para a certificação do âmbito escolhido.	I.Visão executiva dos benefícios II.Velocidades III.Otimização do investimento IV.Planeamento preciso

Tabela 4: Benefícios mais comuns das *framework*

A ISO/IEC 27001:2005 é uma matriz de gestão que permite às organizações a implementação de um Sistema de Gestão de Segurança da informação (SGSI), e a obtenção de uma certificação que

⁵³ SLA (Acordo por níveis de serviço): é um contrato entre um fornecedor de serviço e um cliente, em que ficam descritos os processos de negócio, os serviços suportados, os parâmetros dos serviços, os níveis de aceitação dos serviços, responsabilidade por parte dos fornecedores e acções a serem tomadas em circunstâncias específicas.

reconhece publicamente que a organização possui mecanismos de análise e mitigação dos riscos que afectam a protecção da informação de negócio. Esta norma enquadra-se no grupo de trabalho WG4 - Segurança do ISO/TC 215, e apresenta recomendações que a tornam num guia de conformidade para boas práticas útil para as instituições de saúde, pois é suficientemente flexível para fornecer um conjunto de regras numa “indústria” onde elas não existem. A norma é praticamente neutra em relação à tecnologia, abstraindo-se portanto de sensibilizar a utilização de um sistema de segurança específico em vez de outro. É caracterizada por ser flexível e abrangente para que se possa ajustar aos mais variados ambientes de TI e de forma a ser capaz de crescer dentro de ambientes sujeitos a rápidas mudanças de pessoas, processos e tecnologias. Neste sentido, é expectável que o conjunto de boas práticas induzidas possam levar a organização a apostar na adopção de um modelo de gestão e beneficiar de expectativas de grande, médio impacto e de convergência. Segundo a *tabela 5* apresentada pela *Information Security Forum (ISF)*⁵⁴, segue o impacto médio, grande e de convergência associado à adopção das medidas associadas à introdução de boas práticas ISO/IEC 27002.

Expectativas da implementação de um modelo de gestão baseado em ISO/IEC 27002		
Grande impacto	1	Implementação de boas práticas
	2	Avaliação do estado dos controlos
	3	Definir metas para a segurança da informação
	4	Redução da frequência e impacto de incidentes
Médio impacto	5	Conformidade com as políticas internas
	6	Integração do sistema com o programa ISRM
	7	Ir ao encontro dos requisitos de regulamentação
	8	Maximizar o investimento realizado
De convergência	9	Obtenção de vantagens competitivas
	10	Ir ao encontro dos requisitos da tutela
	11	Adaptar-se às alterações do mercado
	12	Controlo e redução de custos

Tabela 5: Benefícios mais comuns associados à ISO/IEC 27002 (ISF)

⁵⁴*Information Security Forum (ISF)*: é uma organização internacional, independente e sem fins lucrativos que se dedica ao *benchmark* e à identificação de boas práticas no que se relaciona à segurança da informação.

7.3.1. Origem da Norma de Certificação da Segurança

Em meados de Dezembro de 1985 a National Computer Security Center (NCSC) Americana⁵⁵, uma dependência da National Security Agency (NSA), publicou o *Trusted Computer System Evaluation Criteria*, 5200.28-STD, designado *Orange Book*⁵⁶, para o departamento de defesa norte americano (DoD) definindo um conjunto de normas e requisitos elementares de segurança a serem implementados na arquitectura de sistemas de computadores. O *Orange Book* potenciou que fosse criado um centro de avaliação que gerou uma larga quantidade de documentos técnicos e que representaram o primeiro passo na formação de uma norma consensual e completa sobre a segurança de computadores. O *portfolio* de documentos produzidos pelo esforço conjunto dos membros do centro foi reconhecido e denominado de *The Rainbow Serie*⁵⁷, cujos documentos continuam a ser actualizados e estão disponíveis na internet. À medida que as organizações cresceram, as redes de computadores e os problemas de segurança também aumentavam e foi fácil perceber que proteger unicamente sistemas operativos, redes e a comunicação dos dados não seria suficiente. Após a publicação do *Orange Book* emergiram esforços conjuntos globais para a construção de uma Norma, actualizada e que não estivesse focada unicamente na questão da segurança de computadores, mas sim na segurança de qualquer tipo e forma de informação. Foram criados comités que tinham como objectivo o desenvolvimento de mecanismos globais de protecção à informação entre os quais em 1987 o *Comercial Computer Security Centre*, criado pelo Departamento de Comércio e Indústria do Reino Unido (DTI) que veio em 1995 a publicar a norma BS-7799 (*British Standard 7799*) dividida em duas partes a primeira B7799-1 em 1995 e a segunda BS7799-2 em 1998. A BS 7799-1 é a parte da norma desenhada para documento de referência a pôr em execução “boas práticas” de segurança nas empresas; A BS7799-2 é a parte da norma que tem o objectivo de proporcionar uma base para gestão da segurança da informação dos sistemas das empresas (modelo de gestão). A BS-7799 foi a primeira norma homologada a apresentar soluções para o tratamento da informação de uma forma abrangente. Segundo a norma, todo tipo de informação deveria ser protegida, independentemente da sua forma de armazenamento,

⁵⁵ NCSC: National Security Agency/Central Security Service (NSA/CSS) é uma agência da segurança e inteligência do governo dos estados unidos administrada pelo departamento de defesa.

⁵⁶ Orange Book - DoD 5200.28-STD - Trusted Computer. Department of Defense; System Evaluation Criteria

⁵⁷ The Rainbow Series: conhecido como um conjunto de livros de Rainbow são uma série de normas de segurança publicados pelo governo dos estados unidos da américa. Originalmente pelo departamento de defesa dos EUA e mais tarde pela NCSC.

analógica ou digital, e do seu valor para a organização. No final do ano 2000 houve um esforço liderado pela ISO no sentido de elevar a norma BS 7799-1 a uma norma internacional de segurança da informação. Deu-se a união da ISO com a *International Engineering Consortium* (IEC), organização voltada para o apoio da indústria da informação, que tornou a designação da norma com a denominação ISO/IEC-17799:2000. No segundo semestre de 2005 foi lançada uma nova versão da norma, ISO/IEC 17799:2005, que substitui a sua versão anterior e a promulgação e o modelo de gestão é promovido a ISO/IEC 27001:2005, permitindo a criação de um mecanismo de certificação das organizações semelhante às típicas certificações ISO e assegurando que a organização certificada consegue manipular os seus dados e os dos clientes de forma segura, independentemente do local ou forma como estão armazenados (*figura 28*).

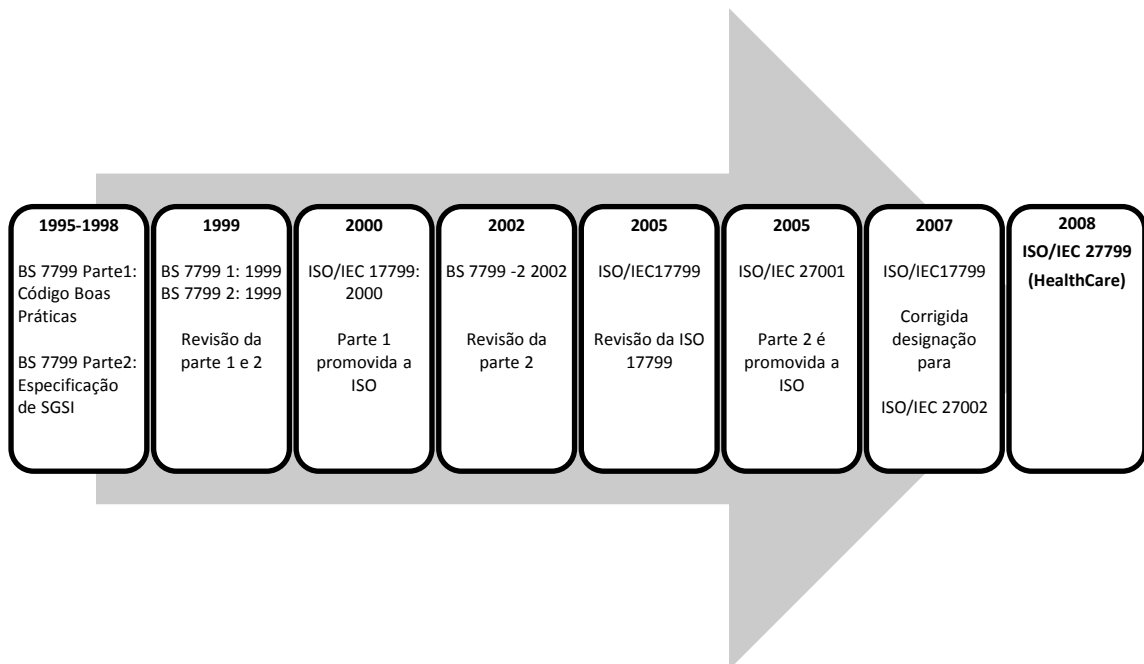


Figura 28: Origem da norma certificadora da segurança para a Saúde

7.3.2. Estrutura da Norma de Certificação da Segurança

De modo a perceber a aplicabilidade da norma ISO/IEC-27002:2005, numa estrutura de interesses e área de actuação, segue a *framework* típica que a compõe com 11 áreas de controlo designadas por cláusulas de segurança (tabela 6)⁵⁸.

	CLÁUSULAS DA ISO/IEC 27002:2005	
1	Política de Segurança da Informação	ISO/IEC-27002:2000
2	Organização da Segurança da Informação	ISO/IEC-27002:2000
3	Gestão de Recursos	ISO/IEC-27002:2000
4	Gestão de Recursos Humanos	ISO/IEC-27002:2000
5	Gestão da segurança física e ambiental	ISO/IEC-27002:2000
6	Gestão das Comunicações e Operações	ISO/IEC-27002:2000
7	Controlo de acessos	ISO/IEC-27002:2000
8	Aquisições, manutenções e desenvolvimento de sistemas	ISO/IEC-27002:2000
9	Gestão de incidentes de segurança da informação	ISO/IEC-27002:2005
10	Plano de gestão da continuidade de negócio	ISO/IEC-27002:2000
11	Conformidade com os aspectos legais	ISO/IEC-27002:2000

Tabela 6: Cláusulas de controlo na norma ISO/IEC 27002:2005

⁵⁸ ISO 27799/2008. INTERNATIONAL STANDARD ISO 27799, First edition, 2008-07-01, Health informatics — Information security, management in health using, ISO/IEC 27002.

7.3.3. A família ISO 27000

A série ISO / IEC 27000 é também conhecida pela família *ISO 27k* que agrega todas as normas da segurança da informação publicadas pela ISO e a IEC, e que vai desde a definição dos vocabulários, requisitos de um SGSI, gestão de riscos, implementação até ao acompanhamento do modelo de gestão e certificação (*figura 29*).

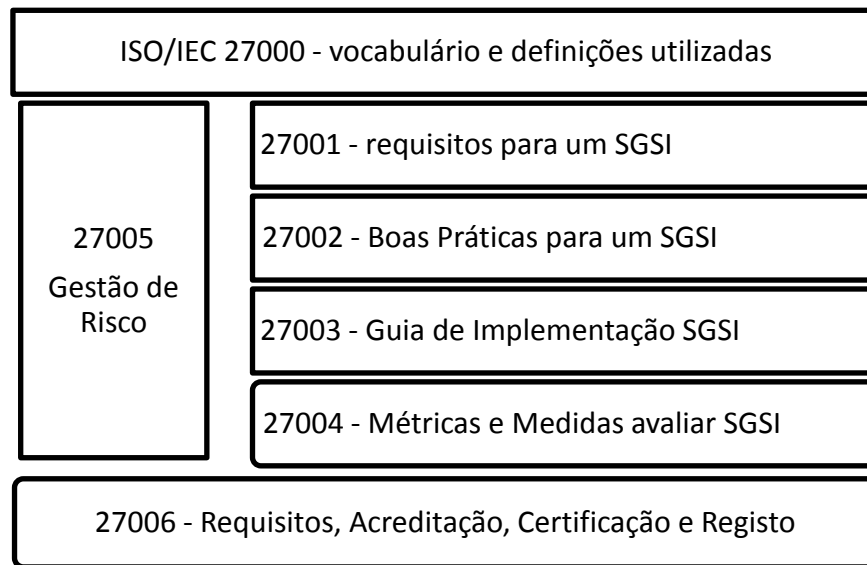


Figura 29: Estrutura de um SGSI

A ISO/IEC 27005⁵⁹ é transversal ao sistema de gestão e totalmente orientada à gestão de risco, que substituiu a antiga parte 3 da ISO/IEC TR 13335:1998⁶⁰. As unidades de medidas identificadas e a pertinência da informação recolhida da estrutura de um SGSI, dão uma orientação clara que vai desde os objectivos que pretendemos alcançar, a forma como podemos chegar até à capacidade de perceber se foram atingidos na totalidade ou em parte (*figura 30*).

⁵⁹ ISO 27005: Componente da serie ISO 27000 e que endereça as normas para a gestão do risco (*information security risk management- ISRM*). <http://www.27000.org/iso-27005.htm>

⁶⁰ ISO/IEC TR 13335-3/1998: Guidelines for the Management of IT Security. JTC 1/SC 27 - IT Security techniques – Part 3: *Techniques for the management of IT Security*. Este capítulo da norma foi substituído pela ISO/IEC 27005.

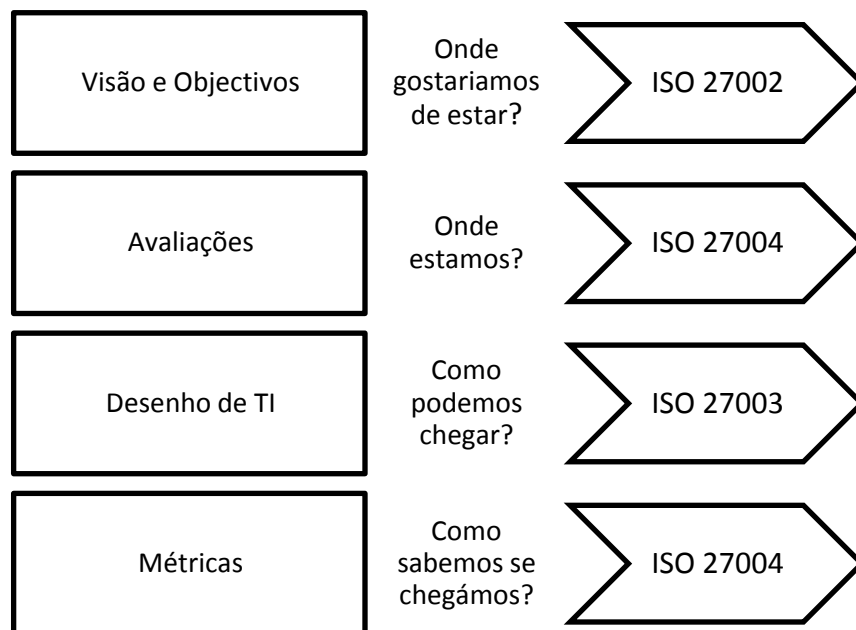


Figura 30: Métricas do SGSI (composição da ISO/IEC 27000)

7.3.4. Importância da norma certificação da segurança

As linhas condutoras para sensibilização do potencial da adopção da norma num organismo de prestação de cuidados de saúde passam pela demonstração de que:

Confidencialidade: Esta propriedade relativamente ao paciente é essencial e fundamental para as actividades relativas à prestação de cuidados de saúde. Cada vez mais os ambientes electrónicos têm vindo a fazer a crescer a preocupação dos pacientes no que respeita à confidencialidade dos dados contidos no seu registo electrónico;

Partilha da informação. O aumento dos acessos à *internet* têm vindo a facilitar a transferência electrónica de documentos de tal forma que existem riscos dessa informação poder ser transferida para locais desapropriados. Para salvaguardar estas situações é essencial a implementação de processos seguros que possibilitem transferência segura da informação;

Abuso ou fraude. Quanto se trata de informação clínica existe este nível de risco associado pelo que para que seja mitigado deve assegurar-se um sistema robusto de gestão da segurança;

Legislação. Tal como existe em outros países da Europa e no mundo, o governo e as instituições públicas deveriam canalizar os seus esforços para alcançar a conformidade na norma e assim obter um reforço à escala nacional no que respeita à utilização segura das redes privadas do ministério da saúde;

Reconhecimento. As organizações de saúde, nomeadamente as grandes e públicas, são naturalmente mediáticas, pelo que a confiança nos sistemas de informação utilizados pode ser um factor de garantia da satisfação dos utentes e adesão a futuros clientes;

A Norma pode facilitar melhor compreensão e o apoio à decisão. Pode ajudar por exemplo disponibilizando de forma segura o acesso a registos clínicos de forma descentralizada, para profissionais e utentes redução de tempos de tratamento e melhores decisões, principalmente quando se tratam de disponibilizar diagnósticos médicos.

7.3.5. Preparação e escolha da metodologia

Para dar início a um processo que permite obter uma visão generalizada da gestão da segurança o recurso responsável por auditar inicia normalmente um processo de avaliação inicial de dados e documentos que confronta com todos os requisitos da norma utilizando para isso uma *checklist* para a recolha clara das políticas, cultura e grau de maturidade sobre a segurança instaurada no ambiente. É com esta avaliação que é possível reconhecer se são suficientes, ou não, o nível de adesão de cada um dos requisitos necessários da ISO/IEC 27002:2005 tais como a privacidade, grau de autenticação dos utilizadores, nível de criptografia nas comunicações ou outros mais críticos para a partir daí se decidir por uma abordagem.

Segundo a norma os resultados de uma avaliação inicial de dados e documentos permitiria à organização:

- Saber em que estágio se encontra em matéria de segurança;
- Reconhecer algumas das vulnerabilidades, ameaças e riscos mais relevantes;
- Delinear um *roadmap* e um âmbito que pode ir até a um projecto de certificação;
- Determinar que recursos e que tipos de plano de projecto se conseguem ter associados.

Assim, a aposta da metodologia para esta dissertação é apoiar os directores dos DSI a elaborar um documento estruturado que resulte num relatório explícito no qual se consiga obter informação que permita reconhecer qual a convergência da organização em relação aos critérios de segurança da informação. Para isso propõe-se a utilização de uma **Avaliação Inicial** de dados e documentos que vamos designar por *Gap Analysis*⁶¹ e que pretende mostrar o nível de adesão, num caso específico de uma instituição prestadora de cuidados de saúde, aos controlos da norma ISO/IEC 27002:2005.

Sujeitos : Processos, Ambientes, Infra-estrutura Tecnológica e Pessoas.

Recursos : Para a elaboração de uma *Gap Analysis* deve estar disponível a documentação necessária da Norma ISO/IEC 27002:2005, ISO/IEC 27001 e ISO/IEC 27799:2008.

Dependendo da sensibilidade da administração do organismo para o que se relaciona com a segurança da informação ou os recursos disponíveis este levantamento pode ser realizado com uma das seguintes combinações de recursos:

- **Gestor da Segurança:** conhecido pelo CISO (*Chief Information Security Officer*) que seria normalmente a pessoa responsável pela segurança da informação no hospital. Este elemento pode ter competências, para além do conhecimento das normas e na gestão de projectos, também alto nível de conhecimentos em gestão e arquitecturas de redes informáticas, políticas de acesso, entre outras;
- **Gestor da Segurança + Auditor Externo:** A alternativa de reforçar na equipa de trabalho um Auditor, externo à organização, pode trazer imensas vantagens associadas à experiência e estatuto do recurso e à sua visão potencialmente mais isenta;
- **Gestor da Segurança + Auditor Externo + Módulo Automatizado:** Esta opção será sempre a mais dispendiosa mas a mais desejada pois garante um projecto com resultados mais rápidos uma vez que é facilitado por um módulo que automatiza a recolha de informação e estrutura o estado das medidas a serem adoptadas no âmbito da norma.

⁶¹ *Gap Analysis*: processo que consta numa avaliação inicial no qual se procura fazer um *site survey* que permita a recolha de vulnerabilidades que estão afectadas os recursos da organização e níveis de risco associados.

Métodos: Segue uma abordagem possível, normalmente utilizada por auditores externos de projecto, para a fase correspondente ao *Gap Analysis* (figura 31).

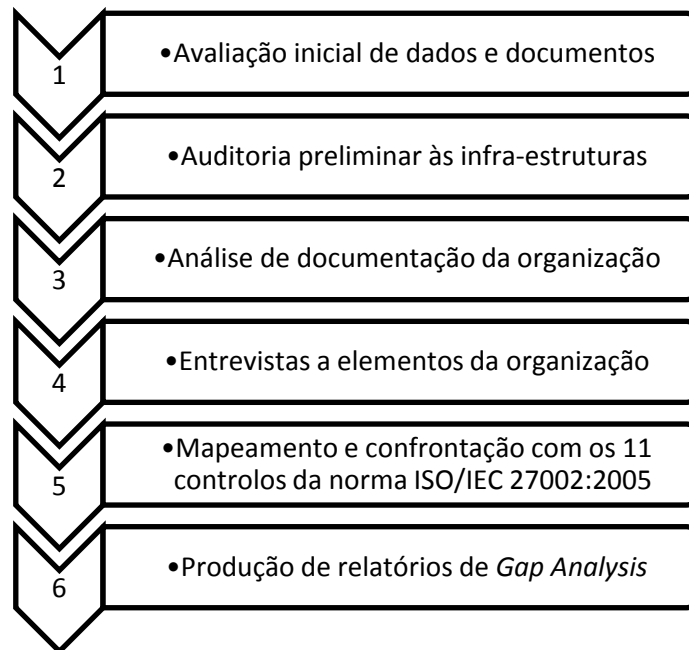


Figura 31: Exemplo de metodologia para uma *Gap Analysis*

A partir dos relatórios de *Gap Analysis*, e em função dos resultados o organismo pode decidir por implementar um modelo de gestão de segurança da informação, contratando para o efeito a colaboração de um *Lead Auditor*, certificado BSI, que normalmente nesta fase já tem orientações e um plano de acção delineado para a adopção de boas práticas com expectáveis benefícios de curto e de longo prazo.

Adopção típica de práticas segundo Alan Calder[19]

- Nomear e divulgar o elemento responsável pela segurança da informação;
- Desenvolver um documento de política de segurança de informação;
- Certificar que todas as aplicações instaladas no hospital processam a informação de uma forma conveniente;

- Gerir incidentes de segurança e promover a melhoria;
- Estabelecer um processo técnico de gestão de vulnerabilidades;
- Garantir formação de segurança, educação e passar conhecimento;
- Desenvolver um processo de continuidade de negócio;
- Ter em conta os direitos pela propriedade intelectual;
- Salvar os registos críticos da organização.

Retorno expectável:

- A redução do risco de incidentes de segurança;
- A redução de custo e do impacto de eventuais incidentes;
- O cumprimento das leis e regulamentos;
- A confiança e credibilidade na prestação de cuidados;
- Um melhor conhecimento dos sistemas de informação e das suas fraquezas.
- Um melhor conhecimento e consciencialização relativamente às questões de segurança, e às responsabilidades de cada colaborador do hospital.

CAPÍTULO VIII

8. APLICAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

8.1. O modelo PDCA (*Plan-Do-Check-Act*)

Tal como já referido, em termos de conceito, existem similaridades na forma de actuação da implementação da norma de certificação de gestão da segurança ISO/IEC 27001:2005 e outras como por exemplo da Qualidade. A ISO/IEC 27001:2005 foi revista de forma a alinhar o mais possível com o modelo típico de utilização do *Plan-Do-Check-Act* (PDCA) utilizado muito no ISO 9001 e ISO 14001. A norma ISO/IEC 27001:2005 é aplicável a qualquer tipo de organização e nelas são especificados os requisitos para o estabelecimento, implementação, operação, monitorização, revisão, manutenção, e melhoria de um modelo documentado de gestão da segurança da informação. Tendo, no contexto da organização, a forma de assegurar a confidencialidade, integridade e disponibilidade dos bens minimizando os riscos. Tal como todos os processos de gestão, um SGSI têm de permanecer a longo prazo como um modelo eficaz e eficiente, e com capacidade de se adaptar às alterações dos processos internos e externos da organização. ISO/IEC 27001 utiliza o PDCA numa aproximação contínua de melhoria (*figura 32*).

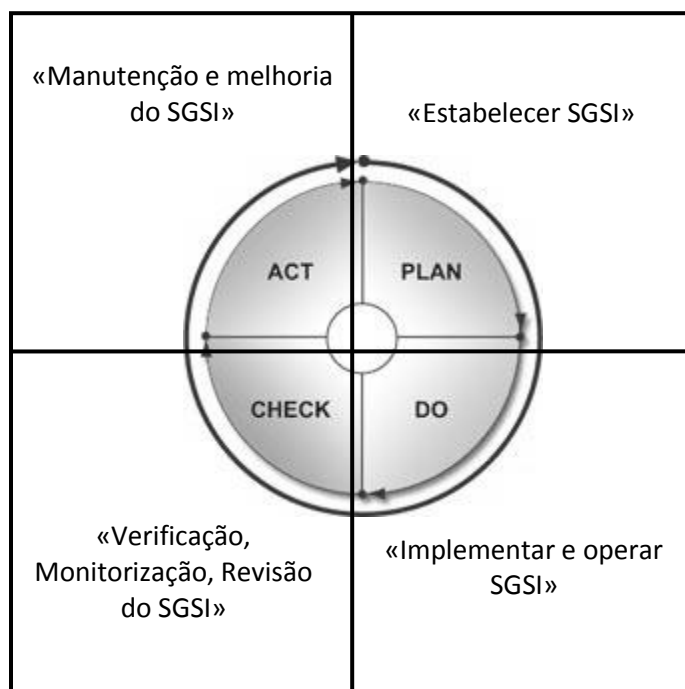


Figura 32: Ciclo de desenvolvimento, manutenção e melhoria

Fase de Planear (*Plan*): desenho do SGSI, no qual são realizados os levantamentos dos riscos de segurança e se seleccionam os controlos apropriados.

1. Definição do âmbito do SGSI;
2. Planeamento das políticas SGSI;
3. Planear a aproximação à avaliação de risco;
4. Identificação, avaliar e planear o tratamento dos riscos;
5. Selecção dos controlos para o tratamento do risco;
6. Preparação do documento “*Statement of Applicability*”, SoA;
7. Aprovação de risco residual e implementação do SGSI.

Fase de Executar (*Do*): implementação e operação de controlos

1. Planear o tratamento do risco;
2. Implementação do plano de tratamento do risco e controlos;
3. Plano de educação e formação;

4. Gestão das operações & recursos;
5. Implementação de registos, controlos e pesquisa de incidentes de segurança.

Fase de Verificar (*Check*): revisão e avaliação do SGSI (eficiência e eficácia)

1. Monitorização de procedimentos e controlos;
2. Revisões sistemáticas ao SGSI;
3. Revisão do risco residual e risco aceitável.

Fase de Agir (*Act*): manter e melhorar o SGSI

1. Implementar eventuais melhorias ao SGSI;
2. Monitorização continua;
3. Comunicações com as partes interessadas;
4. Assegurar que as melhorias atingem os resultados esperados.

8.2. A estrutura do SGSI

Um SGSI é composto pelas 11 cláusulas da norma alinhadas numa determinada estrutura e complementados com mais duas áreas de controlo. Gestão do Âmbito e Gestão de Riscos (*figura 33*).

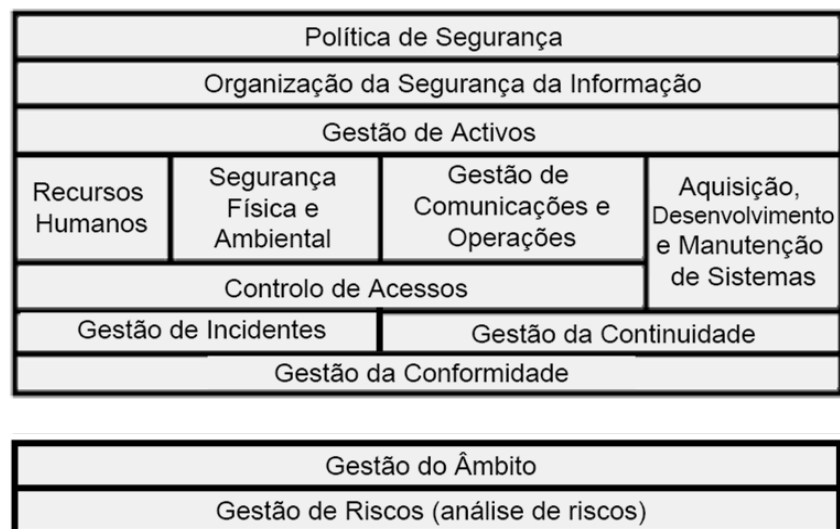


Figura 33: Estrutura de um SGSI

8.3. Processo de desenvolvimento de um SGSI

Mesmo que do ponto de vista da intenção exista uma vontade explícita em adoptar a norma, o sucesso da implementação de um SGSI depende principalmente do envolvimento e aceitação generalizada da organização. O processo de estabelecimento de uma infra-estrutura compatível com as boas práticas da norma pode ser trabalhoso e por isso facilmente o entusiasmo e a dedicação podem esmorecer. O triunfo nessa implementação supõe uma mentalidade e estilo de vida orientado à segurança da informação que deve iniciar a partir da administração da organização. A segurança da informação não é um programa mas sim um processo. Deve ser criada uma base de trabalho para a introdução de um SGSI (*figura 34*) que permita implementar, gerir, manter e seja indutor dos processos de segurança da informação.

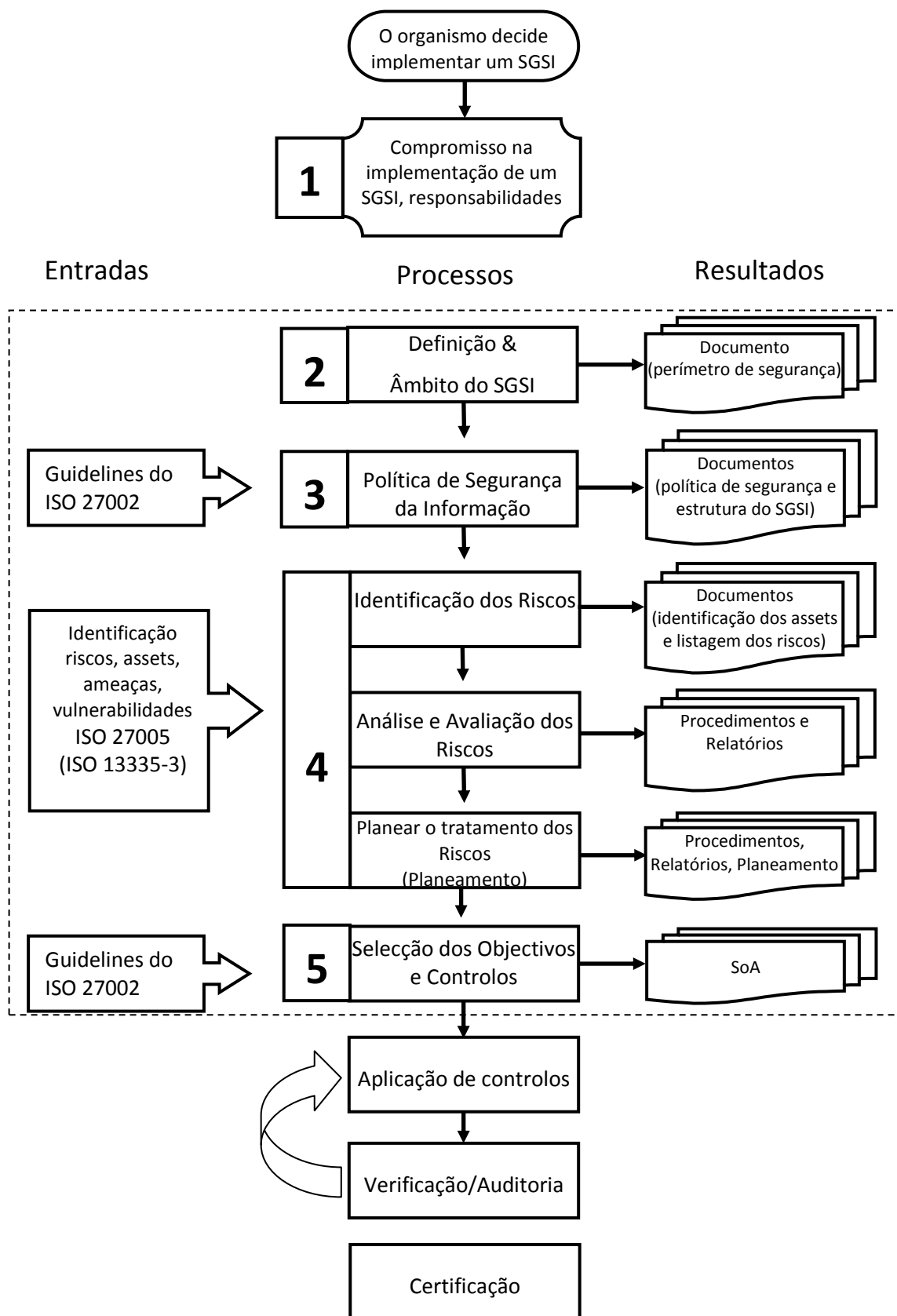


Figura 34: Desenvolvimento de um SGSI segundo a ISO 27001

Segue uma descrição das etapas e sensibilidades a ter na implementação de um SGSI:

Passo1: Compromisso da administração e definição de responsabilidades

A partir do apoio explícito e evidenciado pela administração numa Política de Segurança da Informação o SGSI define o perímetro de segurança e fornece um *roadmap* detalhado com a estratégia para cada uma das áreas de controlo do ISO 27002. Estas estratégias podem ser invocadas para a criação das políticas, normas, procedimentos, planos, comités e grupos ou até contratação de pessoas diferenciadas. De início é importante não só potenciar um líder de segurança (ou um CISO) para coordenar, de ponto de vista macro, a gestão adequada a um SGSI, mas também um fórum de segurança de informação de saúde para estruturar o modelo de governo clínico.

Passo 2: Definição e âmbito do SGSI (perímetro de segurança)

Uma das fases iniciais com maior dificuldade é a definição do perímetro de segurança, ou domínio de segurança no qual se pretende aplicar os controlos. Um perímetro de segurança normalmente pode estar focado na disponibilização segura de serviços de TI seja sobre a infraestrutura como de processos de negócio. O perímetro de segurança pode ou não incluir toda a organização, embora seja obrigatório a organização poder controlar todo o processo. Depois de definido o perímetro de segurança deve ser proposto uma Gap Analysis para uma avaliação de alto nível das desconformidades existentes e que providencia um guia de requisitos de melhoria que dependerá de uma avaliação detalhada do Risco e do modo que será realizado o seu tratamento.

Passo 3: Definição de uma Política de Segurança de Informação

Uma política de segurança da informação pode ter vários formatos. Pode ser um único documento de política global, vários adaptados a várias audiências, ou uma declaração de uma política focada para uma determinada norma. Qualquer modelo terá de ser produzido de forma a mostrar claramente o comprometimento da administração na adopção dessas políticas.

Passo 4: Gestão do Risco - identificar, avaliar, e planejar o tratamento

A aplicação da norma trata com grande incidência uma forma de gerir o risco. Para isso procura-se identificar qual o nível de conformidade com a norma a partir de uma *Gap Analysis* que faça uma avaliação do risco. Só é possível o desenvolvimento de uma estratégia para gerir e mitigar o risco se existir de base um inventário dos *bens* que devem ser protegidos e identificadas as ameaças e vulnerabilidades. Controlos devem ser seleccionados para poder evitar, transferir ou reduzir o risco até um nível aceitável. Uma análise de risco qualitativa é a aproximação à análise de risco mais utilizada. Não são utilizados dados estatísticos mas unicamente uma estimativa de potencial de perda. A maior parte das metodologias que utilizam análise de risco qualitativa fazem uso dos elementos *ameaças*, *vulnerabilidades* e *controlos* de uma forma inter-relacionada. As *ameaças* são eventos que podem ocorrer e atacar um sistema, tais como fogos, inundações, fraudes, etc. e que estão presentes diariamente. As vulnerabilidades tornam os sistemas mais simples de serem ameaçados provocando impacto. Os *controlos* são utilizados como elementos mensuráveis das vulnerabilidades e dividem-se em quatro frentes:

1. Desencorajar: reduzem a possibilidade de ataques deliberados;
2. Preventivos: protegem as vulnerabilidades e podem evitar ataques ou possíveis impactos;
3. Correctivos: reduzem o efeito de um ataque e
4. Detecção: descobrem ataques e activam controlos de prevenção e correcção.

Que podem ser adoptadas do seguinte modo:

- **Identificação dos bens:** Um *bem* pode ser tangível como *hardware* ou intangível como uma base de dados de uma organização. Por definição um *bem* tem associado um valor para a organização e por isso necessita de ser protegido. Os *bens* devem ser identificados e determinado o seu dono. Deve ser atribuído um valor relativo para cada *bem* para que seja dada a devida importância quando os riscos são quantificados.
- **Identificar as ameaças:** as ameaças exploram ou tomam partido das vulnerabilidades dos *bens* para gerar riscos. As ameaças a que cada *bem* está sujeito devem estar identificadas. Cada *bem* pode estar sujeito a várias ameaças. Só as ameaças com probabilidade significativa de acontecer ou de extremo impacto devem ser consideradas (roubo, alteração de uma base de dados, etc.);

- **Identificar as vulnerabilidades:** as vulnerabilidades são reconhecidas como deficiências nos *bens* que podem ser exploradas pelas ameaças para produzir risco. Um bem pode estar sujeito a várias vulnerabilidades (falta de controlo de acesso a uma base de dados ou *backups* insuficientes);
- **Identificar o impacto:** o valor do impacto deve ser quantificado e reflectidos numericamente os prejuízos de uma exploração bem sucedida. Este valor permite uma avaliação numa escala relativa da gravidade de um determinado risco independentemente da sua probabilidade. O impacto não está relacionado com a probabilidade. A avaliação e a mitigação do risco é o principal objectivo de um SGSI. Matematicamente, o risco pode ser determinado com base na probabilidade para cada combinação de ameaça/vulnerabilidade vezes o impacto [31].

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

No qual a probabilidade é determinada pela ameaças cruzadas com as vulnerabilidades e o impacto do ataque é o custo para a organização associado ao *bem* afectado. Esta interpretação numérica permite priorizar com base nos recursos disponíveis, os riscos a mitigar.

A *figura 35* apresenta o efeito das diferentes medidas de segurança e como são relacionadas. O significado deste modelo é apresentar uma estrutura de controlo preventivo que ajude a estruturar conceitos e práticas que desencorajem ataques.

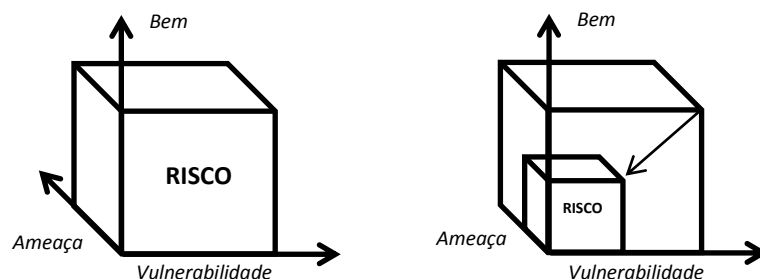


Figura 35: Cálculo de risco - antes e após a aplicação de controlos de segurança

(adaptado de McCumber⁶²) [31]

⁶² John McCumber criou um *framework* que estabelece e avalia a segurança da informação baseado-se numa matriz de *cubo de Rubik* (3 dimensões) e utilizando as propriedades (confidencialidade, integridade e disponibilidade)

Verifique-se na *figura36* a relação entre o risco e o impacto das ameaças para uma organização. Depreende-se que os requisitos de segurança preenchem os controlos que protegem contra as ameaças que exploram as vulnerabilidades dos bens que têm valor para a empresa.

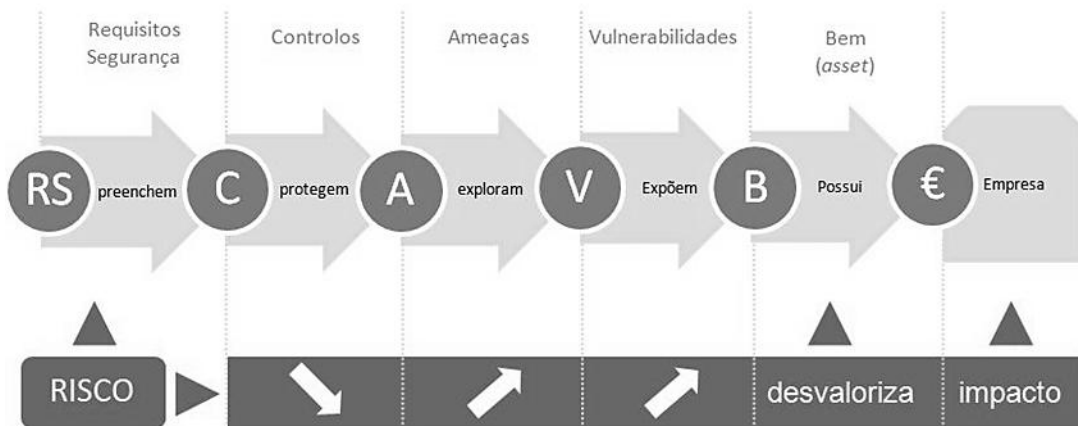


Figura 36: Impacto do risco sobre os bens da organização (adaptada da ISO 27799)

Passo 5: Seleccionar os objectivos e Controlos

O objectivo principal de um controlo de segurança é o de reduzir o efeito conjugado das ameaças e vulnerabilidades à segurança do sistema de informação a um nível tolerado pela empresa. O ideal seria que o controlo fosse capaz de reduzir simultaneamente a probabilidade de ocorrência da ameaça e o seu impacto no negócio (disponibilidade, integridade e confidencialidade). Um controlo devidamente implementado fará diminuir a probabilidade ou o impacto mas até a um determinado limite uma vez que o investimento na aplicação dos controlos pode elevar-se a custos exorbitantes com investimentos sem retorno. Os controlos permitem mitigar os riscos identificados na fase da Avaliação do Risco. Deve ser produzido um documento designado de “*Statement of Applicability*” que é uma parte do SGSI que documenta como os riscos identificados na Avaliação do Risco da Segurança, são mitigados com a utilização dos controlos seleccionados. Este documento endereça as 11 cláusulas de controlo do ISO 27002, e selecciona ou exclui o uso de controlos.

CAPÍTULO IX

9. ESTUDO DE CASO

9.1. Introdução

O papel do Governo das TI (*IT Governance*) seja na sua vertente de Gestão da Segurança (*Security Management*), no âmbito de um Centro de Dados, como o suporte à gestão de serviços de TI (*IT Service Management*), no âmbito do desenvolvimento de um sistema de informação hospitalar, foram considerados como base de dois projectos de *assessment* [32,33] realizados no Hospital São Sebastião em Santa Maria da Feira durante o ano de 2008. A avaliação com base numa *framework* ITIL e em boas práticas de Gestão da Segurança foram essenciais para identificar as fraquezas internas do DSI relacionadas com o governo das TI e despertar para as prioridades a ter não só nas medidas correctivas como também nos investimentos a fazer.

9.2. Caracterização do hospital

O Hospital São Sebastião faz parte de uma rede do Serviço Nacional de Saúde, providenciando serviços de prestação de cuidados de saúde aos utentes da sua referênciação. Está dotado de uma plataforma transversal de software que dá suporte às actividades clínica e administrativas servindo não só a Admissão de Doentes, Consultas e Internamento como também o suporte a outras actividades de ERP⁶³, nomeadamente a facturação. O Processo Clínico Electrónico disponibiliza em regra um interface comum de operação a aproximadamente 320 médicos e 510 enfermeiros que introduzem nos sistemas de informação dados de saúde dos mais variados tipos. Os dados clínicos, nomeadamente os exames de meios complementares de diagnóstico e

⁶³ ERP: *Enterprise Resource Planning*: Conjunto de soluções de suporte à actividade da empresa. Logística, Financeiros, Recursos Humanos, etc.

terapêutica, são arquivados desde 2009 num arquivo concentrado de bases de dados consolidadas.

9.3. Estudo 1 – Gestão da Segurança

Na adopção de boas práticas no âmbito da gestão da segurança é produzido um documento designado de “*Statement of Applicability*” que é uma parte do SGSI e que documenta os riscos identificados e a forma como se pretende que sejam mitigados. O estudo de caso iniciou em 2008 com um trabalho de *Gap Analysis* que permitiu que fossem estabelecido vários controlos de segurança.

9.3.1. Justificação

O Hospital tomou a iniciativa de se envolver neste tipo de aproximação por sentir a necessidade de otimizar alguns processos que sentia não estarem agilizados e seguros nas suas operações nomeadamente na monitorização de acessos dos fornecedores até às políticas de acesso e manipulação de dados de saúde. Uma vez não existindo boas práticas documentadas no âmbito da segurança da informação na organização, antevia-se que uma *Gap Analysis* delimitada ao Centro de Dados, que envolvesse todas as cláusulas da ISO 27002, pudesse resultar em *findings* de importância estratégica a considerar na preservação dos dados de saúde e num plano de continuação da actividade.

9.3.2. Método

O envolvimento da equipa de TI e um grupo que foi criado para endereçar formalmente este levantamento de vulnerabilidades foi mandatário. Depois de algumas pesquisas sobre literaturas relevantes para o assunto em estudo, foi decidido adoptar a *framework* ISO/IEC 27002 (*tabela7*) porque a norma providencia excelentes recomendações para a manipulação de informação crítica, àqueles que são responsáveis em iniciar, implementar ou manter controlos de segurança. Considerações de preservação física e lógica das propriedades da informação como a confidencialidade, integridade e disponibilidade estão reflectidas nas 11 cláusulas da norma. Durante o processo de avaliação da metodologia ponderou-se utilizar o COBIT para endereçar esta avaliação, por ter garantias singulares de que os investimentos a adoptar, estariam alinhados com o que se considera serem os objectivos do hospital. No entanto a sua

implementação exige um envolvimento directo da gestão e outras exigências mais onerosas a nível de implementação que não se traduzem nos objectivos iniciais desta avaliação. A ISO/IEC 27002 está mais focada na eficiência e eficácia dos processos de TI e não num completo alinhamento com os objectivos de negócio do hospital. Esta norma representa um excelente nível de aceitação internacional e está totalmente ajustada às necessidades prementes que visam compreender a que distância está um DSI *per si* de se aproximar ao que se considera serem as boas práticas na gestão dos *bens* da organização.

A metodologia utilizada foi com base no método descrito no capítulo 7 com a seguinte ordem dos trabalhos:

- Avaliação inicial de dados e documentos
- Auditoria preliminar às infra-estruturas
- Análise de documentação da organização
- Entrevistas a elementos da organização
- Mapeamento e confrontação com os 11 controlos da norma (tabela 7)
- Produção de relatórios de *Gap Analysis*

#	ISO 27002 Section
1	Security Policy
2	Organizing Information Security
3	Asset Management
4	Human Resources Security
5	Physical and Environmental Security
6	Communications & Operations Management
7	Access Control
8	Information Systems Acquisition, Development and Maintenance
9	Information Security Incident Management
10	Business Continuity Management
11	Compliance

Tabela 7: Cláusulas para as boas práticas da ISO/IEC 27002

9.3.3. Implementação

O centro de dados da organização concentra todos os servidores aplicativos e de base de dados. Dentro deste âmbito procurou-se realizar uma avaliação (*figura 37*) que permitisse determinar que *bens* compunham esta estrutura de funcionamento e a que riscos estariam sujeitos. Para as vulnerabilidades encontradas foram implementados controlos no âmbito desta infra-estrutura e configurados sobre uma política de segurança que permitiu monitorizar os resultados do processo durante as tarefas do dia-a-dia.



Figura 37: Processo de *Gap Analysis*

As 11 cláusulas que compõem a ISO/IEC 27002 possuem um conjunto de *subsets* baseados nas estruturas da ISO/IEC 27002 e de acordo com uma escala de níveis de risco que especificámos do tipo H-M-L:

H: 76-100% hipótese de ocorrer uma ameaça durante o período de um ano;

M: 26-75% hipótese de ocorrer uma ameaça durante o período de um ano;

L: 0-25% hipótese de ocorrer uma ameaça durante o período de um ano.

O âmbito dos controlos podem ser aplicados de forma que se possa ter uma visão generalizada dos riscos e decidir mitiga-los consoante as prioridades (*tabela 8*).

#	ISO 27002 Section	Risk Level (control objective)		
		H	M	L
1	<i>Security Policy</i>	0	1	0
2	<i>Organizing Information Security</i>	0	1	1
3	Asset Management	2	0	0
4	<i>Human Resources Security</i>	0	1	2
5	Physical and Environmental Security	1	1	0
6	Communications & Operations Management	8	2	0
7	Access Control	5	2	0
8	<i>Information Systems Acquisition, Development and Maintenance</i>	0	4	2
9	<i>Information Security Incident Management</i>	0	2	0
10	<i>Business Continuity Management</i>	0	0	1
11	<i>Compliance</i>	0	1	2

Tabela 8: Níveis de risco e áreas de actuação

As secções que foram consideradas mais críticas, e no qual foram implementados controlos, estiveram ao sob as cláusulas 3, 5, 6 e 7 e no qual genericamente a aplicação de medidas não dependia de intervenção ou participações externas ao DSI. Noutro âmbito e em fase posterior seguir-se-ia um foco de intervenção às restantes cláusulas.

Clausula 3: Asset Management

O objectivo principal do estudo nesta cláusula foi garantir que todos os recursos de informação (*hardware, software, documentos, pessoas, etc.*) utilizados nos processos de negócio a proteger estavam actualizados e eram continuamente inventariados, monitorizados na sua utilização e desempenho, classificados, e devidamente identificados.

- **Pontos críticos encontrados (2):** Os pontos críticos nos quais foram realizadas intervenções estavam relacionadas com a falta de actualização dos bens sobre a responsabilidade do DSI e a ausência de procedimentos instituídos com base em mantê-la actualizada e a falta de definição de quais os recursos mais críticos (*tabela 9*).

Categoria de Segurança	Existem evidências?	Nível de Risco	Categoria mandatória?	Observações
------------------------	---------------------	----------------	-----------------------	-------------

Definição de criticidade para os recursos	Não	H	Sim	Não está definida. Para suporte da análise de risco E continuidade de negócio
Etiquetagem de Recursos de informação	Sim	H	Sim	Não foi garantida a existência de um modelo único de Etiquetagem e de integridade das nomenclaturas utilizadas

Tabela 9: Pontos críticos (cláusula 3)

- **Acção:** Actualização da base de dados de bens físicos, *software* e de *hardware* e procedimento escrito para, no âmbito da gestão de operação, mantê-la actualizada.

Clausula 5: Physical and Environmental Security

Esta cláusula contempla um vasto número de questões relacionadas com a protecção das áreas de trabalho e dos equipamentos que são utilizados para suporte dos processos de negócio a proteger. O controlo de intrusões, detecção e extinção de incêndios, medidas passivas e activas, para garantia de bom funcionamento de equipamentos e dos seus operadores são algumas das acções que endereça.

- **Pontos críticos (2):** Os pontos críticos associados com a segurança física estavam relacionados com a indefinição de perímetros de segurança, e a falta de controlo de acessos junto do *centro de dados* para além das ausências de ronda de vigilância (*tabela 10*).

Categoria de Segurança	Existem evidências?	Nível de Risco	Categoria mandatória?	Observações
Definição de perímetros de segurança	Não	H	Sim	As áreas de segurança não estão definidas nem identificadas
Controlo de acessos físicos	Sim	M	Sim	Apenas na entrada do DSI. Sem controlo do Centro de Dados. Não há controlo Sobre visitantes. Não há rondas de vigilância

Tabela 10: Pontos críticos (cláusula 5)

- **Acções:** Alteração de controlador de acessos para porta do Centro de Dados e solicitação para que rondas de segurança pudessem fazer parte deste perímetro.

Clausula 6: Communications & Operations Management

Esta cláusula é das mais técnicas e abrange temas que vão desde o controlo e monitorização de alterações na rede e nos sistemas até à troca de informações via electrónica e serviços Web.

- **Pontos críticos(10):** Alguns acessos de manutenção externos de vários fornecedores não estavam totalmente identificados, e protocolados. Eram utilizados por regra acessos VPN generalistas (*tabela 11*).

Categoria de Segurança	Existem evidências?	Nível de Risco	Categoria mandatória?	Observações
Monitorização do serviço prestado por terceiros	Não	H	Sim	Não é realizada
Procedimentos de “startup” e “shutdown” documentados	Não	H	Sim	Não existem
Monitorização de sistemas com LOG e Auditoria	Não	H	Sim	Os logs são feitos localmente e não são analisados sistematicamente
Operação documentada de sistemas	Sim	M	Sim	Ausência de documentos formais e de registos de Intervenção manual
Planeamento de alterações	Sim	M	Sim	Não foram apresentadas evidências de documentação de apoio às intervenções
Arquivo e Manuseamento de Tapes em modo seguro	Não	M	Sim	Cofre único e localizado no Datacenter. Não é utilizada criptografia.
Utilização de Correio Electrónico	Sim	L	Sim	Não estará a ser usado para troca de informação sobre o Processo clínico, e não é Monitorizada nem existe qualquer forma de e-mail seguro
Sincronização data/hora redundante	Sim	L	Sim	Em implementação de acordo com recomendações já emitidas
Protecção contra código malicioso	Sim	L	Sim	Inclui Anti-Virus e Anti-Spyware. Mas falta a respectiva política e procedimento de actualização
Plano de <i>backups</i>	Sim	L	Sim	Não foi evidenciada a existência de políticas globais, nem controlo da rotação e arquivo de tapes, nem ensaios de restore

Tabela 11: Pontos críticos (cláusula 6)

- **Acções:** Foram implementados controlos para mitigar os riscos das categorias de *risk level* mais crítico (H). As medidas para suprimir as categorias de *risk level* (M) e (L) ficaram para fase posterior.

Clausula 7: Access Control

Ainda com carácter tecnológico, encontramos nesta cláusula medidas para controlo do acesso a aplicações e bases de dados, gestão de utilizadores e respectivas palavras passe, utilização de equipamentos portáteis e acessos remotos.

- **Pontos críticos (7):**A falta de identificação e de classificação da informação para além da ausência de políticas para o manuseamento de equipamentos informáticos foram as evidências mais críticas encontradas nesta cláusula (*tabela 12*).

Categoria de Segurança	Existem evidências?	Nível de Risco	Categoria mandatória?	Observações
Circulação interna de informação em modo seguro	Não	H	Não	Uma vez que não está identificada nem classificada a informação não é possível de momento comentar
Política de “Clear Screen”	Não	H	Não	Não existe, apesar dos PCs bloquearem automaticamente
Utilização de portáteis em modo seguro	Não	H	Não	Não existe política correspondente nem medidas adequadas
Utilização de acesso remoto	Sim	H	Sim	Não existe qualquer documentação de autorização e e monitorização
Alteradas as passwords por “default” nos recursos	Não	H	Sim	Sem sempre está a ser realizado
Utilização de telemanutenção	Sim	M	Sim	Não existe qualquer documentação de autorização e e monitorização
Politica para gestão de passwords	Sim	L	Sim	Existe uma politica em fase de aprovação.

Tabela 12 : Pontos críticos (cláusula 7)

- **Ações:** Foram implementados controlos para mitigar os riscos das categorias de *risk level* mais crítico (H). As medidas para suprimir as categorias de *risk level* (M) e (L) ficaram para fase posterior.

9.4. Estudo 2 – Gestão de Serviços de TI

9.4.1. Justificação

O DSI do hospital, tal como na generalidade dos departamentos dos hospitais, estão perante problemas que surgem devido à grandes mudanças no sector nomeadamente a necessidade de introdução de sistemas clínicos, de suporte à actividade assistencial e de apoio. Seja por falta de

pessoas qualificadas até devido a uma desapropriada priorização nos investimentos a verdade é que as maiores dificuldades encontram-se a nível da gestão de projectos, gestão operacional e da segurança da informação, com consequente desalinhamento de uma estratégia global para as TI. O objectivo do *assessment* ITIL no hospital foi para ajudar a identificar lacunas relacionadas com a utilização das TI e perceber a que distância estaria a organização de poder ultrapassá-las.

9.4.2. Metodologia

A norma ISO/IEC 38500 disponibiliza princípios básicos para a uma utilização apropriada dos recursos de TI de acordo com base na *framework* de Calder-Moir⁶⁴, que se compõe em seis princípios: *responsabilidade; estratégia; aquisição; desempenho; conformidades e comportamento humano*. Uma vez que a *framework* é demasiada extensa, o estudo incidiu na componente ao nível de gestão de serviços (*IT Service Management*) optando pelas questões relacionadas com o *Service Desk* e o *Incident Management*, que são mais do que suficientes, para que do ponto de vista operacional, se possam encontrar as fraquezas do DSI.

9.4.3. Implementação

O processo de *assessment* em ITIL iniciou-se de modo a tentar apurar até que nível o hospital conseguiria suportar iniciativas de mudança de melhoria nos processos. Procurou-se *gaps* das estruturas e das pessoas a começar pelos papeis e responsabilidades dos colaboradores não só do DSI como também de outros Serviços desta unidade. Para ajudar a fazer o levantamento dos papeis dos colaboradores e das suas responsabilidades foi utilizada a matriz RACI (*Accountable, Responsible, Consulted, and Informed*)⁶⁵ que permitiu clarificar e cruzar as funções com as responsabilidades (*figura 38*).

⁶⁴ Calder-Moir: http://www.itgovernance.co.uk/calder_moir.aspx. Acedido a 10/04/2010

⁶⁵ RACI: Authority Matrix for clear definition of accountability and responsibility. Is a critical success factor for any process improvement project, including the implementation of best practices according to ITIL.

	Role A	Role B	Role C	Role D
Function / task 1	R	A	C	I
Function / task 2	A	R	C	I
Function / task 3	C	R		A
Function / task 4	R	C	I	A
Function / task 5	I	A	R	

Figura 38: Exemplo de matriz RACI

No primeiro levantamento de funções verificou-se que embora o CIO não fizesse parte integrante da administração do hospital, no que se relaciona ao governo das TI existia um grande alinhamento com os objectivos de negócio do hospital. Ainda nessa fase de avaliação verificou-se que os SI/TI suportam toda a estrutura da cadeia de valor do hospital (*figura 39*), o que revela um indicador do potencial acréscimo de valor destes sistemas e qual a sua importância no contexto da organização.

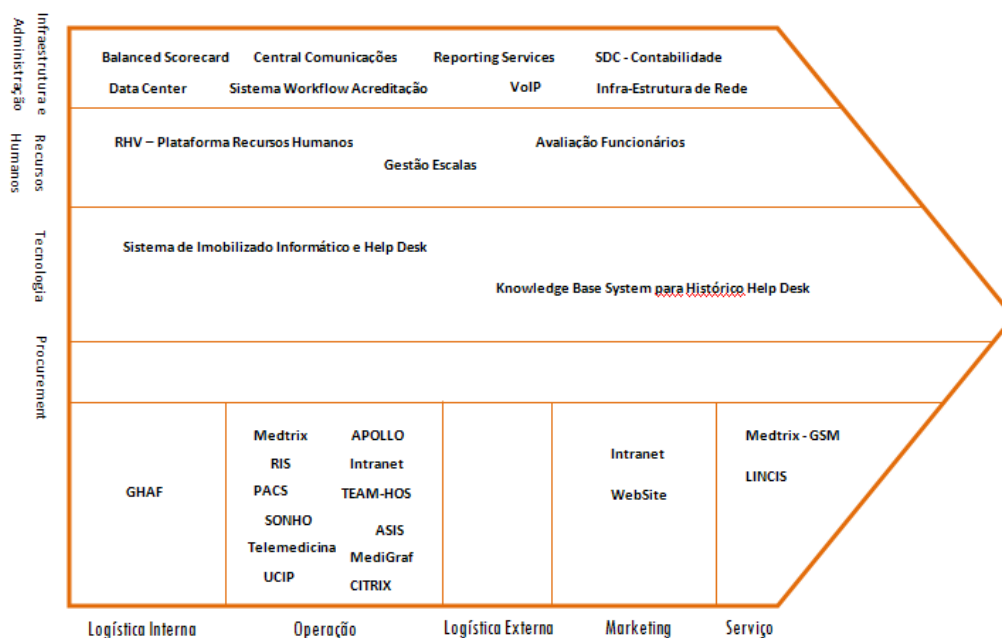
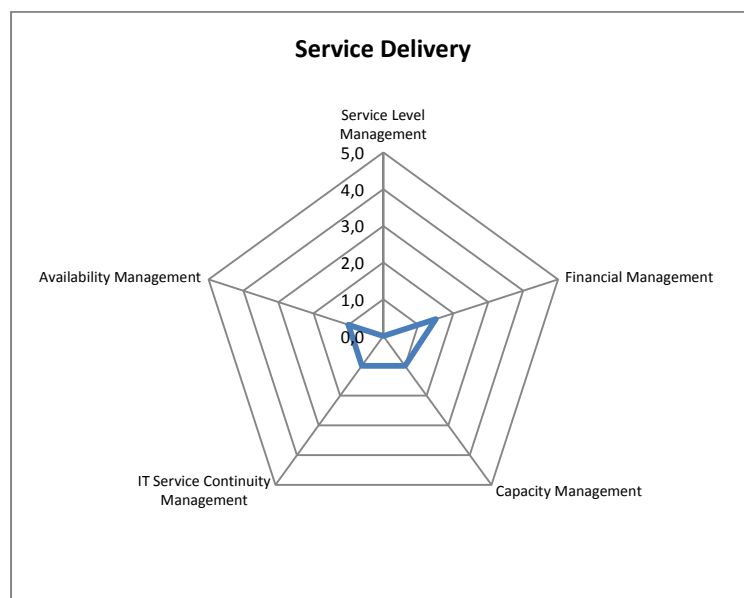


Figura 39: Aproximação a um modelo de cadeia de valor dos SI/TI do hospital

O DSI possui uma ferramenta para o registo de actividade de *service desk* e para a gestão das incidências mas que parece não estar a ser retirado todo o seu potencial. Tendo por base os dados desta solução e para apurar a maturidade de boas práticas ITIL no DSI, foram produzidos questionários OGC⁶⁶ que foram respondidos pelo CIO e que foram analisados de forma a comparar que a informação recolhida estava de acordo com as evidências recolhidas no terreno (*figura 40*).



⁶⁶ ITIL OGC: *Self assessment questionnaire*. Direitos da itSMF.

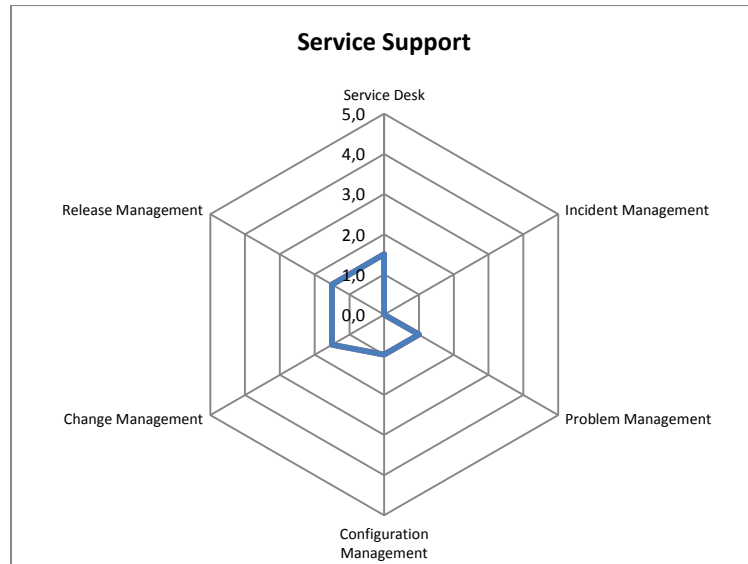


Figura 40: Nível de maturidade *IT Service Management*

Como podemos constatar o nível de maturidade tanto de *Incident Management* e *Service Level Management* não atinge o nível 1 ficando com nível de maturidade mínima que é “zero”. Significa que os processos serão realizados de uma forma *had-hoc*, sem grande definição e planeamento e através de aproximações esporádicas. Uma aposta na componente de *Incident Management* traria benefícios expressivos e ganhos rápidos e o facto de ter o mínimo grau de maturidade não é aceitável para um DSI e muito menos numa organização deste tipo. A solução de suporte a relatos de incidentes não é utilizada na íntegra para o tratamento de todos os incidentes nomeadamente os mais críticos que são resolvidos e comunicados unicamente por telefone. Os utilizadores do sistema de informação são os primeiros a justificar que a qualidade de resposta a pedidos não é eficiente. Detectou-se que do DSI qualquer colaborador poderia exercer *helpdesk*, e isso não contribui para a resolução do problema. Optou-se portanto, aprofundar a análise relativamente à gestão das incidências.

Um incidente é qualquer evento que não fazendo parte de uma operação de rotina, quando ocorre pode causar uma redução de Qualidade de Serviço. O principal objectivo da gestão de incidentes é garantir a reposição desse serviço o mais rapidamente possível mitigando os riscos associados a esse restabelecimento e eliminando o mais possível os efeitos colaterais.

Para esta análise foi utilizado o método de Steinberg⁶⁷ que considera no processo de análise 4 P(s): *Processos, Pessoas, Produtos e Performance* e que permitem estruturar informação de forma a mapear tanto a componente de *Service Desk* como de *Incident Management* numa *framework* de maturidade ITIL⁶⁸ (Figura 41).

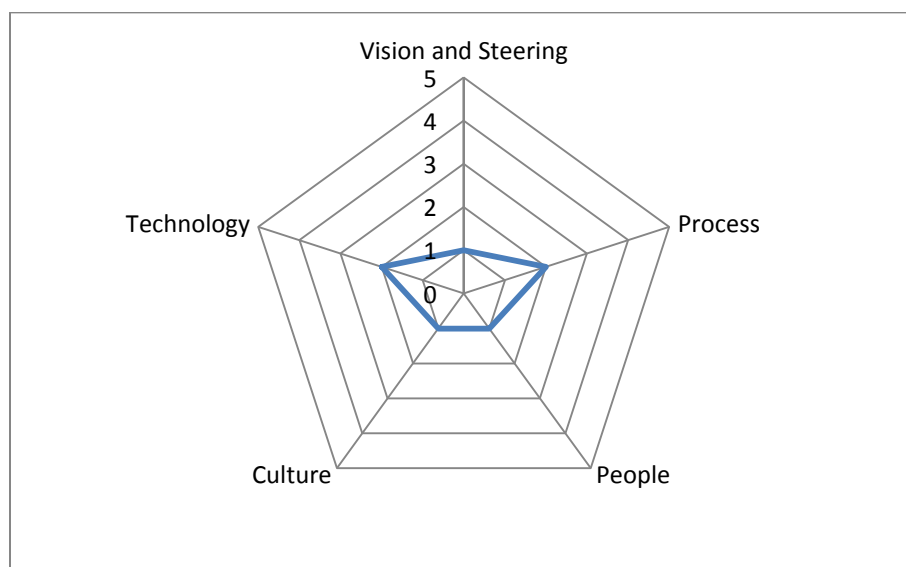


Figura 41: *Incident Management Maturity Framework (PMF)*.

Podemos verificar que a tecnologia e os processos são as rubricas com grau de maturidade 2 no que respeita ao *Incident Management*. As rubricas *Vision & Steering*, *Pessoas* e *Cultura* estão assinaladas com grau de maturidade 1. Uma vez que o DSI necessita de tomar medidas para superar as dificuldades nas questões relacionadas com chamada a incidentes, e tendo constatado que do ponto de vista tecnológico e de processos já estão no nível 2, significa que o trabalho a realizar terá de ser no âmbito das pessoas/organização, cultura ou noutras formas de gestão.

⁶⁷ Steinberg, R.A. (2008) *Implementing ITIL: Adapting Your IT Organization to the Coming Revolution in IT Service Management*.

⁶⁸ ITIL Process Maturity Framework

Com base neste pressuposto foi produzida uma matriz designada por modelo RACI (*Accountable, Responsible, Consulted, and Informed*) que mapeia numa única estrutura as funções, competências e responsabilidades das equipas que compõem o DSI (*figura 42*).

ID	Function	ID	Function
1	Department Administration and Management	8	User's Training
2	User Support/Help Desk	9	Project Management
3	Network and Communications Management	10	Procurement and Stock Management
4	Database Management	11	Innovation
5	Applications Management and Support	12	Probationers Coordination
6	Clinical Applications Development	13	Informatics Prevention
7	Support Applications Development	14	Business Interaction

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
CIO	A/R	R	A/R	I	A/I	C/I	C/I	A/R	A/R	A/R	A/R	A/R	A/R	A/R
Network Manager	C/I	R	R		R			R	R		R		R	R
Project Manager	C/I	R	R	R	R	A	A	R	A/R/I		R	R	R	R
Technician 1	C/I	R			R				C/I					
Programmer 1	C/I	R		C/I	R	R								R
Database Manager	C/I	R	R	A/R	R	R	R	R	R/C/I	R	R		R	R
Support DB Manage	C/I	R		R	R		R	R	R/C/I					R
Programmer 2	C/I	R		C	R	R	R	R	R	R	R	R	R	R
Programmer 3	C/I	R			R	R	R	R	C/I					R
Programmer 4	C/I	R			R	R	R	R	C/I					R
Technician 2	C/I	R			R				C/I					

Figura 42: modelo RACI de funções e responsabilidades

Esta matriz revelou que existe um grande nível de funções em *overlap* entre os colaboradores que apontam para ineficiências nas questões de *IT Service Management*. Pode verificar-se que qualquer colaborador do DSI pode ser responsável por funções de *helpdesk*, inclusive o CIO uma vez que também é responsável por operar um grande conjunto de funções nomeadamente de gestão de projectos.

9.5. Conclusões

Durante o projecto de gestão da segurança pudemos verificar que houve uma intenção clara de não indiciar a análise nas duas primeiras cláusulas da norma. A cláusula primeira e segunda que são *Política da Segurança* e *Organização da Segurança da Informação* respectivamente foram deixadas para fase posterior uma vez que dependiam muito de um explícito comprometimento

e disponibilidade do Conselho de Administração que por essa altura não era possível beneficiar. Assim, o Director do DSI optou por iniciar o processo de *Gap Analysis*, sobre as cláusulas mais tecnológicas, fazendo depender o sucesso do *assessment* inteiramente da sua equipa.

Com base nestes casos de estudo podemos concluir que para além da necessidade de se promoverem internamente códigos de prática para a gestão da segurança da informação, também ao nível da gestão de serviços existem ineficiências que são uma barreira ao desenvolvimento dos sistemas de informação hospitalares.

O *IT Service Management* tem imenso impacto no dia a dia nas actividades dos prestadores de cuidados de saúde. Em ambos os casos as investigações realizadas são parte de um programa bem mais vasto e estruturado que deveria acontecer na condicionante de não se virem a proporcionar as medidas de correcção necessárias. Esse programa seria uma abordagem sistémica aos sistemas de gestão que poderiam vir a ser implementados para cada um destes modelos. Eles têm orientações diferentes que importa dar relevo para perceber como se complementam (*tabela 13*).

SGSTI	SGSI
Orientado ao Serviço	Orientada ao Risco
Garantir a entrega de Serviço de acordo com os requisitos e os níveis de serviço acordados com base em • Disponibilidade • Performance	Garantir a segurança da informação relativamente ao seus requisitos de • confidencialidade, • integridade • disponibilidade
Dentro das TI	Transversal à organização

Tabela 13: Comparação entre os dois modelos de gestão.

A abordagem a um modelo de gestão orientado aos serviços de TI (SGSTI) é totalmente orientada ao Serviço, está delimitada pelas TI e pretende garantir a entrega de serviços de acordo com os requisitos e o níveis de serviço acordados com base na *disponibilidade* e *performance*. A abordagem a um modelo de gestão focado na segurança da informação (SGSI) já

está mais orientado ao Risco, é transversal à organização, e pretende garantir a Segurança da Informação com base nos indicadores de *confidencialidade, integridade e disponibilidade*.

CAPÍTULO X

10. ENSAIO DE RESPOSTA AOS PROBLEMAS COLOCADOS

10.1. Interpretação dos Resultados

A garantia das conformidades da ISO/IEC 17799:2005 e a certificação da norma ISO/IEC 27001, por si só, não garante que o hospital ficou 100% seguro. Na verdade, a não ser que se evite toda e qualquer actividade na organização, cenário irrealizável, não vai existir nunca a segurança total. No entanto, a adopção destas normas internacionais proporciona vantagens do ponto de vista das *garantias*, aspectos *operacionais*, de *negócio* e *humanas* que não devem ser desconsideradas:

Garantias – a certificação assegura, a todos os níveis, utilidade e proveitos retirados do esforço colocado pelo hospital na segurança e reflecte da administração do hospital uma imagem de competência;

Conformidades – a certificação demonstra às entidades competentes que o hospital reconhece e faz por aplicar as leis, regulamentos e boas práticas (exemplo orientações da Comissão Nacional da Protecção de Dados);

Operacional – a gestão do risco leva-nos a compreender melhor o comportamento dos sistemas de informação, os seus pontos fracos e a melhor forma de os proteger. De igual forma assegura uma relação de maior “confiança” *hardware* e dados.

Negócio – deste ponto de vista existe mais credibilidade e confiança dos parceiros, utentes, *stakeholders* em geral e reconhecerão nos investimentos realizados, as vantagens atingidas com os níveis de protecção da informação. A certificação destaca nitidamente o hospital dos seus “concorrentes” para além de que no âmbito da Europa a legislação já convida os organismos públicos e privados a se posicionarem estrategicamente nas conformidades com a norma.

Custos – com a gestão da segurança existe uma redução significativa dos custos comparados com a iniciativas que tendam a implementarem a segurança da informação de uma forma *ad-hoc*.

Humanos – a iniciativa favorece a formação e conhecimento necessário para os funcionários estarem convictos e sensíveis aos tópicos da segurança e quais as suas responsabilidades dentro do hospital.

Na teoria o nível de segurança atinge o nível de maturidade adequado quando for completamente discreto. Podemos dizer que o sistema de gestão da segurança está saudável logo que ninguém se lembrar da sua existência. No entanto, se for ocorrer um constante desconforto pelos utilizadores por exemplo por falhas nos acessos ao *email*, aplicações, *internet*, demasiado *spam* ou políticas aborrecidas que obrigam constantemente os utilizadores a alterarem as palavras passe então é porque ainda existe um longo caminho a percorrer na implementação dos mecanismos de gestão da segurança da informação.

10.2. Ensaio de resposta aos problemas colocados

No capítulo 2 foram levantadas questões, que ao longo da investigação foi possível consolidar respostas que ajudam a perceber os benefícios que estarão subjacentes a uma aposta nos modelos de governação que apoiam a protecção da informação de negócio. Segue um ensaio de resposta às questões levantadas nesse capítulo.

- *Quais serão as melhores práticas para implementar a Gestão da Segurança na minha organização?*

Ensaio de Resposta: As melhores práticas para assegurar efectiva gestão da segurança da informação são feitas com base na implementação de um sistema de segurança de gestão da informação (SGSI). A ISO/IEC 27001 foi revista de forma a alinhar o mais possível com o modelo típico de utilização *Plan-Do-Check-Act*. O SGSI é o resultado da aplicação de um conjunto de objectivos, orientações, políticas, procedimentos, modelos e outras medidas administrativas que de uma forma global definem como são reduzidos os riscos para a segurança da informação. A implementação da norma 27001 constitui *per si* um SGSI.

- Qual é o melhor processo de avaliação dos riscos e como se pode e deve implementar?

Ensaio de Resposta: O método utilizado neste estudo para a avaliação e gestão do risco foi com base na ISO 27005 no qual a metodologia é composta por 5 fases: avaliação; tratamento; aceitação; comunicação; monitorização e revisão dos riscos de segurança da informação. No entanto existem inúmeros métodos, e que são divulgados por duas organizações que enumeram e comparam os vários métodos existentes na indústria:

A ENISA publica no seu sítio *web*⁶⁹ 12 ferramentas com 22 atributos distintos que permite fazer comparações com outros métodos e ferramentas existentes (*figura 43*), e a ISECT Ltd. disponibiliza informações de mais de 50 métodos para a gestão do risco num repositório *web* indexado à ISO 27001⁷⁰.

Figura 43 : Ferramenta ENISA para comparações diferentes métodos de Gestão de Risco

⁶⁹ Ferramenta da ENISA para comparação entre diferentes métodos de gestão de risco. <http://rm-inv.enisa.europa.eu/comparison.html>. Acedido a 08/04/2010

⁷⁰ www.iso27001security.com/html/faq.html#RiskAnalysis. Acedido a 08/04/2010

- *Quais as melhores práticas de protecção dos recursos de informação da empresa?*

Ensaio de Resposta: As melhores práticas são baseadas numa *framework*. O modelo ISO/IEC 27002 e as cláusulas que a compõem são uma boa ferramenta para assegurar efectiva gestão de segurança da informação, mesmo que não exista qualquer interesse da organização em certificar o âmbito escolhido;

- *Como podemos comparar os esforços de protecção da informação na organização com o melhor que a indústria tem para oferecer?*

Ensaio de Resposta: A ISO 27799:2008 está focada na saúde e é baseada na ISO 27001 que está sustentada nas práticas do modelo ISO 27002, amplamente adoptado em qualquer indústria.

- *Como se pode extrair visibilidade dos investimentos aplicados em segurança e qual o retorno para a minha organização?*

Ensaio de Resposta: A adopção e comprometimento de uma organização para qualquer modelo de gestão de segurança da informação, expõe de uma forma clara o interesse da instituição em proteger os seus bens de negócio e assim dar credibilidade interna e externa aos seus *stakeholders*. A adopção de boas práticas exige *per si* que os ambientes tenham por exemplo os bens inventariados, valorizados e controlados e a identificação das ameaças e os valores de perda a que podem estar sujeitos. Todo o desenvolvimento de um SGSI induz a uma redução de desperdícios, optimização de processos de trabalho com ambientes de trabalho controlados.

10.3. Tendências e Investigação de futuro

Previsões

Os investimentos em curso nas empresas são por regras promovidos por um gestor responsável em gerir financeiramente o projecto. Provavelmente foi avaliado o retorno de investimento dos projectos, em termos de benefícios directos ou indirectos, que a empresa pode obter. Por

sensibilidade as regras do mercado parecem dizer que um lucro não é mais do que o cálculo das receitas deduzido das despesas. A segurança da informação era por regra vista como uma despesa o que era pouco saudável. Assim, por regra os investimentos na segurança eram vistos como despesas adicionais e que podiam comprometer os lucros da empresa. No entanto esta tendência está a desvanecer e as despesas que actualmente são contabilizadas nas empresas também incluem perdas de produtividade, desperdícios por horas no restabelecimento de sistemas sujeitos a ataques ou devido a manutenções deficitárias ou negligentes. Deste modo a tendência das empresas já tem vindo a orientar-se na avaliação dos benefícios reais que as apostas na segurança induzem. Desde 22 de Março 2005 que tinha sido publicado um regulamento europeu onde se percebia claramente quais as tendências da União Europeia relativamente às políticas da segurança da informação. Segue o exemplo de uma directiva em relação à protecção dos interesses financeiros das comunidades onde o regulamento (CE) 465/2005 que destina avaliar, com a norma ISO/IEC 27001, a conformidade da segurança dos Sistemas de Informação relativo ao financiamento da política agrícola comum (*Department of Agriculture, Fisheries and Food*). No relatório anual de resultados de 2008 do departamento de agricultura comum (*Annual Output Statement*) [34], no qual se definem objectivos até 2010, essas directivas continuam a fazer parte explícita dessa estratégia (*figura 44*).

Outputs	
2007 Output Target	2007 Output achieved
.....	
5.4. Ensure a stable, robust secure ICT infrastructure and provide on a timely basis the necessary information systems to support our operations, as verified by the EU Paying Agencies' Certifying Body and the achievement of the service delivery targets in the CSAP and the Charter of Rights for Farmers.	The timely delivery of the range of departmental schemes and payments indicated in Goal 4 above together with the fact that our ICT systems experienced no significant operational down time in 2007 is concrete verification that our ICT systems and infrastructure are stable, robust and support all DAFF operations. In addition, ICT system security management is specifically audited by the EU Certifying Body, (using the Capability Maturity Model) on the 11 domains outlined in ISO 27001 Standard: Code of Practice for Information Security Management. They have verified that in 2007 DAFF has maintained to a high standard the formal structures and processes required.

Figura 44: "2008, *Annual Output Statement*". Departamento de agricultura da União Europeia

Investigação de futuro

Ao longo de mais de 10 anos convivendo com a temática associada à Segurança da Informação e infra-estruturas TIC em organismos de saúde, foi possível observar a evolução das tecnologias, bem como a maturidade dos processos relativos aos SI dos hospitais públicos em Portugal. Verifica-se que cada hospital se encontra num grau de maturidade diferente seja da cultura, processos e de estrutura dos seus SI. E embora se possa esboçar ou utilizar um modelo típico comparativo de avaliação da maturidade, a realidade é que mesmo os hospitais no qual a dignificação desta actividade é alta e até existe uma estratégia alinhada com os objectivos de negócio, a segurança não é uma prioridade. Também a ausência de incidentes graves, não fez despertar as direcções do DSI para a necessidade destas iniciativas, pelo que seria desejável que não se tivesse de esperar até esse extremo. A proposta de continuidade desta investigação passa pela disponibilização, a um conjunto de hospitais públicos, da *framework* em anexo que serve tipicamente para apoiar uma avaliação inicial que ajude a dar um “pontapé de saída”, para que se possa apurar o estado de arte, no que respeita ao risco e vulnerabilidades associadas aos *bens* da organização. Com base nessa análise o organismo pode reagir adoptando os controlos que se ache prioritários. A compilação dos resultados anonimizados desse estudo iria apurar de uma forma bem mais realista o estado de arte e maturidade das TIC dos hospitais e outros organismos do Serviço Nacional de Saúde.

CAPÍTULO XI

11. CONCLUSÕES

A realidade demonstra que nenhuma organização estará algum dia totalmente protegida das ameaças que põem em risco a Informação vital para o negócio. E muito menos os organismos de saúde com a grande diversificação de actividade assistencial, no qual a disparidade de sistemas de informação e a interacção com fornecedores de serviços é acentuada e de complexidade óbvia. Investir num nível de protecção que se considere próximo do ideal atingiria custos muito elevados ou bloquearia de forma não aceitável os processos desenvolvidos pelo hospital. Pode-se mesmo afirmar que, com a excepção do caso extremo, em que se cessa toda a actividade, não existe o cenário de segurança total. O que um SGSI possibilita é uma abordagem sistemática dos riscos e a implementação de controlos com o objectivo de os minimizar. A adopção de todos os controlos da ISO/IEC 27002 por si só não garantem um nível de certificação. A certificação só é garantida com a a ISO/IEC 27001 que é a referência de excelência da Gestão da Segurança da Informação através da qual é possível certificar um sistema. A aplicação da norma certificadora permite gerir ou conhecer o estado de arte, relativamente a segurança, mas em nenhum momento me garante a segurança e daí a necessidade de introduzir controlos da ISO/IEC 27002. Quanto à adesão da utilização da norma no âmbito do SNS, a não ser que alguma entidade reguladora do Ministério da Saúde um dia promova e ajude a financiar uma certificação deste tipo, dificilmente qualquer administração de um hospital estará sensível a investir num processo de certificação que à partida exige algum investimento e comprometimento e que implica grandes mudanças estruturais no âmbito das tecnologias e nos comportamentos. No entanto, e tal como já acontece com alguns países da Europa, a norma provavelmente nos próximos anos

será implícitamente de carácter obrigatório uma vez que é a única que certifica a segurança, e porque a complexidade e a insegurança crescem exponencialmente sendo cada vez mais difícil manter a segurança tendo em vista a diversidade de sistemas e utilizadores. Daí, este estudo ter incidido na adaptação de uma *framework* para uma *Gap Analysis* que pudesse apoiar uma gestão das TI, numa avaliação inicial do estado de saúde dos seus *recursos*, com vista a procurar níveis de riscos associados, e poder-se activar medidas de gestão para o controlo eficaz dos processos críticos. A estruturação destes dados, numa forma sistematizada, ajudaria a retratar o estado do hospital em matéria de Segurança da Informação e seria como uma ferramenta de *check up*, e modelo de actuação, com vista à melhor preservação da informação crítica do hospital.

GLOSSÁRIO

BS7799:	Norma britânica de segurança da informação que deu origem ao ISO/IEC 17799.
BS7799-1:	Primeira parte da BS7799, que teve sua primeira versão homologada no ano de 1995
BS7799-2:	Segunda parte da BS7799, que teve sua primeira versão homologada no ano de 1999
BSI:	<i>British Standards Institute</i> . Primeira entidade britânica a emitir normas a nível nacional. É um dos membros fundadores da Organização Internacional de Normalização (<i>International Organization for Standardization</i> - ISO)
BASILEIA II:	Esta é a nova versão de um conjunto de princípios essenciais desenvolvidos pelo Comité de Gestão Bancária para a supervisão bancária.
CIO	<i>Chief Information Officer</i> . Designação de responsável máximo pela direcção de gestão das tecnologias e dos sistemas de informação numa organização
CISO	<i>Chief Information Security Officer</i> . Designação de responsável máximo pela segurança da informação numa organização
COBIT :	O CobiT é um guia para a gestão das TI orientada ao negócio da organização.
CTO	<i>Chief Technological Officer</i> . Designação de responsável técnico gestão das tecnologias e dos sistemas de informação numa organização
DOD 5200.28-STD :	É a sigla oficial do Orange Book;
FIREWALL	Hardware ou software utilizado para aumentar os níveis de segurança de uma rede local ou abrangente.
ISO	A <i>International Organization for Standardization</i> , é uma entidade internacional responsável pela emissão de normas técnicas e pelo

processo de certificação das organizações;

ISO 14001	Norma internacional, que estabelece parâmetros de implementação e operação de um sistema de gestão ambiental;
ISO 15408	Conhecido por <i>Common Criteria</i> é uma norma voltada para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras;
ISO/IEC 17799	Norma internacional de segurança da informação;
ISO 27799	Versão da norma ISO 27001 adaptada em 2008 para a saúde;
MALWARE	Abreviatura de pedaço de software desenvolvido para se infiltrar num sistema operativo sem que o utilizador seja informado ou autorize.
NCSC	O <i>National Computer Security Center</i> , é uma parte da estrutura da agência nacional de segurança dos Estados Unidos que é responsável por testes de segurança;
NIST	O <i>National Institute of Standards and Technology</i> é um dos órgãos norte americanos responsáveis pela emissão de normas técnicas
NSA	O <i>National Security Agency</i> , este é a agência norte americana de segurança que publica guias de segurança para vários sistemas operativos nomeadamente <i>Windows</i> , <i>Novell</i> e <i>Linux</i> ;
ORANGE BOOK	Este foi a designação dada à primeira versão do documento que originou a norma de segurança BS7799;
RAINBOW SERIES	É o conjunto de documentos produzidos pelo Departamento de Defesa dos EUA (DoD)
HACKERS	Ou Cracker é o indivíduo que acede sem direitos de acesso a um sistema de informação contornando o sistema de segurança

BIBLIOGRAFIA

- [1] UMIC - Sociedade da Informação e do Conhecimento. “Inquérito à Utilização das Tecnologias da Informação e da Comunicação pela Comunidade Portuguesa nos Hospitais”, 2004. Disponível em <http://www.unic.pt> [consultado em 04/02/2009]
- [2] UMIC - Sociedade da Informação e do Conhecimento. Relatório à Administração pública Central. (2006). “Inquérito à Utilização das Tecnologias da Informação e da Comunicação”. Disponível em <http://www.unic.pt> [consultado em 03/07/2009]
- [3] SYMANTEC REPORT 2007. “Relatório de Ameaças à Segurança na Internet”. Disponível em http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf [consultado em 20/04/2010]
- [4] Número de certificados ISO/IEC 27001 por país. Disponível em <http://www.iso27001certificates.com> [consultado em 26/02/2010].
- [5] Finne T., (2000). “Information systems risk Management: Key concepts and business processes.” Computer & Security, 19 (3) 2000.
- [6] Deloitte. “Security Survey 2007”. Disponível em http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf. [consultado em 26/04/2010].
- [7] CIO. (2010). “Home Land Security. Pick Up two”. Disponível em http://www.cio.com/article/10517/Homeland_Security_Cheap_Fast_or_Secure_Pick_Two, [consultado em 15/03/2010]
- [8] ENISA. (2007). “Prática corrente e avaliação do sucesso Julho de 2007”. Disponível em <http://www.enisa.europa.eu>. [consultado em 15/04/2009]
- [9]] Mai, J-E. (2005). “The Many Dimensions of Information. Information School University of Washington”.

- [10] Pfleeger, P.C., Lawrence, S., et al. (1997), "Security in Computing", third ed., Prentice-Hall, 2003
- [11] Parker, D., et al (1995), "A new framework for information security to avoid information anarchy". Proceedings of IFIP TC11, 13th international conference on Information Security.
- [12] Ferreira, A. (2002). "Electronic Patient Record Security". IS9 Project, MSc in Information Security, Information Security Group
- [13] Ferreira, A., Correia, R-J, Antunes, L., CHADWICK, D. "Access Control: how can it improve patients' healthcare?" Disponível em <http://www.icmcc.org/pdf/2007/2007ferreira.pdf>. [consultado em 11/02/2010]
- [14] Ferreira, A., Correia, R-J., Chadwick, D., Santos, H., Gomes, R., Reis, D., Antunes, L., (2008). "Password Sharing and How to Reduce It". FMUP.
- [15] Irish League of Credit Unions . "Report of the National Technology Committee ICT Strategy 2007-2011". Disponível em http://www.ilcu.ie/files/20070426020620_ICT%20Strategy%20-%20Summary%20Report..pdf. [consultado em 10/05/2010].
- [16] Media Capital. (2007). "Relatório sobre o Governo da Sociedade". Disponível em <http://web3.cvm.pt/sdi2004/emitentes/docs/RGS17455.pdf>. [consultado em 15/04/2009]
- [17] OCDE. (2004). "Os Princípios da OCDE sobre o Governo das Sociedades". Disponível em <http://www.oecd.org/dataoecd/1/42/33931148.pdf>. [consultado em 15/01/2010]
- [18] Calder, A., Watkins, S., et al. (2006). "International IT Governance: Na Executive Guide to ISO 17799 / ISO 27001". Kogan Page
- [19] Harvard Business School. (2004) "Ten Principles of IT Governance". Disponível em <http://hbswk.hbs.edu/archive/4241.html>. [consultado em 15/01/2010]
- [20] ISACA. Information Systems Audit and Control Association. (1999). "Information Security Policy". Disponível em <http://www.isaca.org.za>, [consultado em 11/01/2009]
- [21] DTI. Departamento de Comércio e Indústria Britânico. (2006). Disponível em <http://www.dti.gov.uk/files/file28343.pdf>. [consultado em 12/03/2009]

- [22] Spafford, G. Garfinkel, S. et al. (2002), "Web Security, Privacy & Commerce", 2.^a ed., O'Reilly.
- [23] Zachman Framework. (1987). "Zachman International web page". <http://zachmaninternational.com/>
- [24] Lapao L.V. (2007). "Survey on the status of the hospital information systems in Portugal". *Methods of Information in Medicine*; 46 (4): 493-499. [Original article indexed in ISI and Scopus]
- [25] Morin, E. (1991). "Introdução ao Pensamento Complexo", Ciências Sociais na perspectiva da Complexidade (17/19)
- [26] BERR. Department of Business Enterprise and Regularoty Reform. (2008). "Information security breaches survey". Disponível em [http://www.pwc.co.uk/pdf/BERR_ISBS_2008\(sml\).pdf](http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf). [consultado em 10/03/2009]
- [27] Entrust. (2006). "Information security breaches survey" em colaboração com a *PriceWaterHouseCoopers, WC, Microsoft, Symantec, Entrust e ClearSwift*. Disponível em <http://www.entrust.com/resources/pdf/information-security-breaches-survey.pdf> . [consultado em 10/05/2010]
- [28] CNPD. (2004). "Relatório de Auditoria ao Tratamento da Informação de Saúde nos hospitais", disponível em http://www.cnpd.pt/bin/relatorios/outros/Relatorio_final.pdf. [consultado em 10/05/2010]
- [29] Holland, M. (2008). "HealthCare IT Maturity; Drivers & Barries. EMEA vc. The US". CIO Summit, Evian, France.
- [30] CALLIO. "Nível de risco pela exposição de um sistema de informação por sector de actividade". Disponível em <http://www.callio.com/bs7799>. [consultado em 27/07/2007]
- [31] McCumber, J. (2005). Et al. "Assessing and managing security risk in IT systems: a structured methodology". Auerbach.

[32] Gomes, R. J., Lapão, L.V. et al. (2008). "The Adoption of IT Security Standards in a Healthcare Environment." eHealth Beyond the Horizon – Get IT There S.K. Andersen et l. (Eds.) IOS Press, MIE 2008

[33] Lapão, L. V., Rebugue, A., Silva, M.S., Gomes, R. J. "ITIL Assessment in a Healthcare Environment: The Role of IT Governance at Hospital São Sebastião". Medical Informatics in a United and Healthy Europe K.-P. Adlassnig et al. (Eds.). IOS Press

[34] FEOGA. (2008). "Annual Output Statement. 2007". Disponível em <http://www.agriculture.gov.ie/media/migration/publications/2008/AOS2008Englishversionoflrishttranslation.doc>. [consultado em 27/02/2010]

ANEXO A

Interpretação e adaptação às cláusulas

(Rui Gomes)

INTERNATIONAL STANDARD ISO 27799, First edition, 2008-07-01,

Health informatics — Information security, management in health using, ISO/IEC 27002,

Informatique de santé — Gestion de la sécurité de l'information relative, à la santé en
utilisant l'ISO/CEI 27002

Clausula 1- Política de Segurança da Informação

O primeiro objectivo apresentado na norma é a elaboração de um documento formal para as políticas de segurança da informação. A política de segurança clarifica aos funcionários qual o nível de comprometimento da administração e da estrutura da organização em geral com a gestão da segurança da informação e a forma como esta deve ser tratada. É uma declaração simples que apresenta a informação como parte do negócio, um bem valiosíssimo e que deve ser preservado por exemplo com a definição de procedimentos para assegurar, a confidencialidade dos registos clínicos sejam em papel ou em formato electrónico. Especificamente num hospital será o gestor da segurança em articulação com a administração e a gestão intermédia a elaborar um plano de gestão onde conste uma declaração de intenções quando se pretenda a partilha de informação. Esta política deve estar também de acordo com os aspectos legais ou orientações da tutela em vigor para a manipulação de dados clínicos. Devem estar também definidas políticas para a descrição de procedimentos para a gestão da continuidade de negócio e *disaster recovery* caso a instituição seja sujeita a acidentes, desastres, ou outras intempéries.

Clausula 2- Organização da Segurança da Informação

Existe necessidade de identificar as pessoas e qual o seu papel e responsabilidades no envolvimento na estrutura da informação da organização. Quais os níveis de acesso e privilégios deverão ter por exemplo cirurgiões, médicos, enfermeiros, técnicos entre outros. Os hospitais normalmente estão envoltos numa rede diferenciada de prestação de cuidados de saúde onde é necessário recorrer à troca de informação entre as instituições da rede. Será necessário que simples trocas de registos clínicos tenham de ser asseguradas por uma infra-estrutura robusta e segura e que afiance também um procedimento seguro de troca de informação. A relevância da restrição de acessos quando se trata de entidades externas é da maior importância. Fornecedores, subsistemas financeiros, empresas contratadas para telemanutenção, etc. lidam diariamente com os hospitais e com informação dos doentes numa dinâmica que obriga a muita troca de informação entre ambas as partes. Esta clausula incentiva que seja utilizado um espírito da segurança a ser partilhado com estas instituições.

Clausula 3- Gestão de Recursos

O objectivo desta cláusula é assegurar a protecção adequada dos bens da organização, vulgarmente conhecidos por *assets* (bens tangíveis ou inatingíveis). Os serviços médicos e outros deverão poder gerir e ter um registo actualizado dos recursos do seu serviço (inventário) dos seus bens associados e dos sistemas de informação utilizados. Tudo deve estar inventariado. Bases de dados com informação de utentes, *backups*, inventário de medicamentos, etc. e todo e qualquer software que é utilizado para o registo e pesquisa desta informação também deve estar inventariado. O acesso à informação associada a estes bens, uma vez que é sensível, também deve ser controlada.

Clausula 4- Gestão de Recursos Humanos

Esta cláusula pretende reduzir o risco do erro humano, roubo, fraude ou abuso de utilização dos bens da organização nomeadamente a importância do acesso à informação clínica. A título de exemplo, nos hospitais existe uma grande quantidade de pessoas com um papel preponderante na manipulação da informação quando relacionados na distribuição de processos clínicos em papel ou electrónicos. Os estatutos dos colaboradores que utilizam essa informação documentos devem ser verificados tal com a credibilidade das qualificações que apresentam nomeadamente em instituições que requerem um grande nível de profissionalismo e responsabilidade. Este tipo de responsabilidade deve ser considerada também quando se opta pela subcontratação temporária seja de profissionais como das empresas externas responsáveis pela prestação de serviços de cuidados de saúde, enfermeiros, médicos, técnicos etc. Nestes casos, pode acontecer a necessidade de salvaguardar com confidencialidade as situações contratuais desses profissionais.

Clausula 5- Gestão da segurança física e ambiental

A partir desta cláusula estaremos com condições de utilizar pontos de controlo para assegurar a inibição de acessos não autorizados a informação sensível. Essa informação deve estar localizada em local seguro e sujeita a premissas de controlo de acesso. Arquivo de dados dos doentes, registos de funcionários de todas as categorias profissionais (médicos, auxiliares, técnicos, enfermeiros, etc.). Devem existir também acessos físicos restritos aos registos dos laboratórios e aos meios complementares de diagnóstico e terapêutica (MCDT) em geral de forma a assegurar a integridade, segurança e confidencialidade dessa informação. Verifique-se por exemplo alguns controlos de grande relevância:

- Controlo físico de acessos (internamentos, blocos, urgência, outros locais de acesso, etc.);
- Segurança nos quartos e instalações principalmente nos lugares onde se encontre informação sensível como os registos de pacientes e relatórios médicos devem estar inacessíveis a pessoas não autorizadas e afastados de instalações povoadas de pessoas como por exemplo zonas de fotocopiadoras, *faxs*, entre outros;
- As áreas de fornecimento de bens como aprovisionamentos, lavandarias devem estar afastadas o mais possível de áreas de prestação de cuidados do hospital;

A segurança dos equipamentos é um outro ponto importante principalmente durante um processo de prestação de cuidados até porque a informação será guardada em diversos equipamentos médicos, computadores, etc. e daí a necessidade de minimizar o risco de fuga de informação. Ter em consideração que a informação clínica realizada em cópias redundantes, para auxiliar o tratamento do doente, deve ser convenientemente descartada logo que não seja necessária.

Clausula 6- Gestão das Comunicações e Operações

Esta cláusula está orientada a potenciar uma comunicação segura da informação minimizando a probabilidade de falha nos sistemas. Este elemento da norma deve garantir que o formato dos dados deve ser o mais apropriado para a comunicação dos dados entre os profissionais. Procedimentos e manuais de operações devem ser utilizados para sensibilizar os utilizadores como podem utilizar os equipamentos informáticos e outros recursos disponíveis. Devem ser preparadas técnicas para gerir e reagir a incidentes de segurança como por exemplo o desvio de processos clínicos, violação de acessos, entre outros. A criação de planos de contingência é fundamental pois só assim se pode potenciar continuamente o funcionamento de serviços de qualidade na prestação de cuidados de saúde. A separação de funções e responsabilidades é também uma boa técnica para reduzir o risco da má utilização dos sistemas por falta de competências. Por exemplo os actos de prescrição e administração de medicação aos pacientes são claramente duas actividades com competências separadas nas quais a separação destas garante mais segurança que a informação a tratar é devidamente interpretada e gerida evitando a possibilidade de erros graves. Permite-se criar uma barreira que evita actividades de fraude. Os acessos às redes informáticas, entre a maior parte das instituições de cuidados de saúde, estão a crescer exponencialmente pelo que controlos de gestão desta informação nomeadamente as ameaças de vírus, *spam*, entre outros é uma componente que deve ser tida em consideração. Outros factores que devem ser considerados na gestão das comunicações são as trocas de formulários com informação crítica e que devem ser quantificados na política tais como os diálogos públicos sobre o estado dos pacientes ou *post its* em lugares públicos, e outros.

Clausula 7- Controlo de acessos

Clausula para uma política de controlo de acessos deve ser definida e documentada. Uma vez que diferentes grupos profissionais necessitam de diferentes tipos de informação e as permissões de acessos também variam, esses privilégios devem ser revistos regularmente por um administrador de sistemas. Devem ser utilizadas *firewalls* seja de *hardware*, *software* ou até de pessoas e a encriptação de ficheiros para que se possa evitar acessos não autorizados. Ter em conta a gestão das palavras passe para controlo da informação sensível e o controlo da computação móvel no qual por vezes os profissionais de saúde levam para o exterior, sem critérios, registos com informação de saúde.

Clausula 8- Aquisições, manutenções e desenvolvimento de sistemas

Trata-se de uma cláusula que permite assegurar que os requisitos de segurança da informação são incorporados nos desenvolvimentos seja de serviços como de processos. Testes e controlos deverão ser verificados para garantir a integridade e a autenticidade dos dados. Ferramentas como a encriptação e os certificados digitais podem ajudar a proteger os dados. A tecnologia pode ajudar por exemplo para estabelecer um mecanismo de não repudição de mensagens através da utilização de processos como por exemplo *date stamping* [56]. Isto pode ajudar por exemplo no preenchimento electrónicos de formulários com informação clínica sensível nos relatórios médicos como os certificados de nascimento e morte.

Clausula 9- Gestão de incidentes de segurança da informação

A gestão de incidentes só apareceu na versão da norma de 2005 e contempla a comunicação de eventos de segurança da informação, comunicação de falhas de segurança da informação, responsabilidades e procedimentos. Esta cláusula sugere que sejam implementadas medidas direccionadas para sensibilizar a aprendizagem, recolha e registo dos incidentes de segurança da informação (colecção de incidências).

Clausula 10- Plano de gestão da continuidade de negócio

Em serviços públicos como hospitais, centros de saúde, etc. que são pólos de excelência numa infra-estrutura local ou nacional da prestação de cuidados de saúde, é essencial que existam processos implementados de modo a proteger qualquer de qualquer interrupção as actividades críticas de negócio. Os processos devem ser mapeados de modo a assegurar-se a continuidade de serviços, mesmo em caso de desastres onde existam por exemplo motivos de falha no sistema de comunicação de voz entre paramédicos, ambulâncias, situações de emergência ou então falhas de energia nas consultas externas, blocos operatórios ou nas urgências. Aos profissionais de saúde que são chave devem ser dadas responsabilidades para desenvolverem os seus planos de continuidade de negócio. Cada sector de um hospital deve estar representado no fórum de segurança interno.

Clausula 11- Conformidade com os aspectos legais

A violação das leis e contratos ou o não cumprimento destes são tidos, do ponto de vista da opinião pública e entidades tutelares, como uma falta de compromisso e desconsideração à Qualidade. As áreas médicas, técnicas ou de enfermagem possuem um conjunto de orientações profissionais com códigos de conduta e regulamentos que devem ser considerados para uma boa gestão de cuidados aos doentes. O hospital tem a responsabilidade de assegurar estas componentes e seguir esses códigos de conduta sejam os de carácter clínico como de manuseamento de equipamentos, higiene, saúde e segurança.

Para a certificação da segurança da informação (ISO/IEC-27001:2005) é necessário dirigir esforços para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI). Segue a estrutura da norma ISO/IEC 27000 e o valor que está associado a cada uma das normas (*figura 29*).

ANEXO B

FRAMEWORK PARA RECOLHA DE DADOS EM LABORATÓRIO (GAP ANALYSIS)

(Rui Gomes)

Política da segurança da informação

Políticas existentes no hospital	Existem Políticas S/N	São divulgadas fora da organização S/N	Observações
Segurança informática			
Segurança da Informação (ISO/IEC 27002)			
Qualidade (ISO/IEC 9001)			
Ambiente (ISO/IEC 14000)			
Higiene, Segurança e Saúde Ocupacional (OHSAS 18000)			
Outras...			

Organização de Segurança

Gestão estratégica e operacional de segurança	Existe? S/N	Qual a finalidade prevista?	Observações
Compromisso formal da Administração			
Coordenador de Segurança			
Acordos de confidencialidade com funcionários ou colaboradores internos			
Acordos de confidencialidade com entidades e/ou colaboradores externos			
Gabinete de auditoria			
Recurso a contratação externa de serviços SI/TI			
Recurso a contratação externa a serviços de segurança			
Outros...			

Gestão de Recursos

Classificação, Identificação e Inventário	Existe? S/N	Descrição	Observações
Existe um inventário global dos recursos que existem no hospital? (listagem ou ficheiro)			
Existe uma identificação dos recursos críticos para com o negócio? (servidores, UPS, ligações WAN, telefones, fax, recursos humanos)			
Estão identificados quais os recursos indispensáveis para o hospital caso surjam inundações, fogos, etc.?			
Existe internamente a figura do “responsável do recurso”? Ou seja cada recurso crítico identificado ter um responsável associado.			
Existe algum modelo de etiquetagem dos recursos que são utilizados no hospital.			
Existe alguma classificação interna da informação ou método de classificação? (Informação confidencial, publica, etc...)			

Gestão de Recursos Humanos

Gestão de Recursos Humanos	Aplicável? S/N	Quantidade	Descrição	Observações
Existem definições para a responsabilidades dos funcionários nas suas actividades dentro e fora do hospital?				
O serviço de gestão de Recursos Humanos participa na gestão de acessos e credenciais de acesso a recursos pelos funcionários				
Existe um manual de acolhimento ao funcionário? O que tem de relevante em termos da segurança?				
Existe um plano de formação no hospital? Inclui a realização de acções de segurança?				
Quantos são os recursos humanos no hospital com acesso a informação crítica?				
Quantos funcionários pertencem ao Departamento de Sistemas de Informação?				
• Operação de sistemas				
• Redes e Comunicações				
• Desenvolvimento				
• Gestão de base de dados				
• Suporte às aplicações				
• Gestão da Segurança				

Segurança Física e Ambiental

Segurança física e ambiental	Existe S/N?	Quantidade	Descrição	Observações
Quantos os edifícios compõem o hospital				
Quantos serviços são críticos?				
Quantas zonas críticas identificadas (gabinetes direcção, <i>datacenter</i> , UCI, Bloco, etc.) ?				
Portarias para identificação dos visitantes?				
Existe sistema de controlo de acessos com registo histórico?				
Sistema de detecção de incêndio? Existe nas zonas críticas?				
Sistema de extinção de incêndio? Existe nas zonas críticas?				
<i>Outsourcing</i> de manutenção de <i>hardware e software</i> ?				
Existem base de dados instaladas por entidades externas ao qual o hospital não possui a estrutura de dados e nem tem forma de acesso directo às tabelas de dados?				
Existem sistemas de videovigilância? Abrange as zonas críticas?				
Existe vigilância contratada para os edifícios que compõem o hospital?				
Existem UPS transversais ou departamentais?				
Existem grupos de energia alternativa?				
Existe estudo para avaliação de impacto de sismos?				
Existem sistemas de controlo das condições ambientais com histórico de temperatura de humidade (<i>datacenter</i> , Blocos operatórios, câmaras frigoríficas de medicamentos, etc..)				

Gestão das comunicações e operações

Gestão das comunicações e operações	Existem procedimentos documentados para gestão de.. S/N	Existem recursos humanos dedicados para a gestão de.. S/N	Existem registos de.. S/N	Observações
Operação de sistemas				
Planeamento de alteração na rede de sistemas, comunicações e seerviços				
Separação de ambientes de testes e desenvolvimento				
Monitorização da utilização de TODOS os recursos das entidades externas				
Monitorização da prestação de serviço das entidades externas				
Protecções contra código nocivo				
Backups de dados				
Politica e procedimento de backup com manuseamento de tapes				
Gestão da segurança das redes (wired e wireless)				
Serviços de correio electrónico				
Monitorização de sistemas com recursos a logs e auditoria				
Consola central para a gestão de eventos e alertas				
Sincronização de hora/data na rede de serviços				

Controlo de acessos

Gestão de acesso à informação	No acesso lógico à informação S/N	No acesso físico à informação S/N	Observações
Controlo no acesso à informação de gestão (UserID, Passwd, biometria, impressão, cartão magnético)			
Documentação de uma política de <i>passwords</i> (troca de x em x dias, mascara, etc...)			
Processo documentado para abertura de utilizadores na infraestrutura informática			
Processo documentado para anulação/bloqueio de utilizadores na infraestrutura informática (cessação de contrato de trabalho)			
Sistema de <i>Single Sign On/SSO</i> (<i>one user one passwd</i>) permitem o acesso a vários recursos.			
Existem registos de autorizações de acesso a informação de negócio?			
A circulação interna da informação física é efectuada de forma segura (processo clínico, prescrições, etc..)			
Existe uma política de <i>harning</i> (<i>clear desk, clear screen</i>)			
Existem PC portáteis em actividades de negócio? É permitida a utilização no exterior do hospital?			
Existem acessos remoto a sistemas e aplicações pelos funcionários			
Existe acesso remoto a sistemas e aplicações por empresas externas?			
São utilizados armários seguros ou cofres para salvaguardar informação de negócio?			
Existe política definida para o tipo de informação a armazenar em local seguro?			

Aquisição, desenvolvimento e manutenção de sistemas de informação

Aquisição, desenvolvimento e manutenção de sistemas de informação	Existem procedimentos documentados para a gestão de... S/N	Existem elementos dedicados para a gestão de... S/N	Existem registos de...	Observações
Especificação e análise de requisitos de segurança para o desenvolvimento de sistemas.				
Especificação e análise de requisitos de segurança para a aquisição de sistemas				
Validação do processamento e resultados de aplicações crítica				
Utilização de cifra para aplicações críticas				
Controlos para o processo de desenvolvimento de sistemas aplicativos.				

Gestão de incidentes de segurança da informação

Gestão de incidentes de segurança de informação	Existem procedimentos documentados para a gestão de... S/N	Existem elementos dedicados para a gestão de... S/N	Existem registos de...	Observações
Serviço de <i>HelpDesk</i> interno				
Serviço de <i>HelpDesk</i> externo				
Identificação de vulnerabilidades				
Criação de registos de vulnerabilidade por sistemas e colaboradores				
Análise e classificação de incidentes de segurança gestão de incidentes e medidas correctivas				

Gestão da continuidade de negócio

Plano para continuidade de negócio	Elemento responsável pela análise e planeamento	Definição dos recursos críticos necessários para sobreviver a acidente?	Identificação de papéis a desempenhar em caso de acidente?	Observações
Processos críticos de negócio				
Definição dos níveis de risco aceitáveis e de medidas para tratamento de risco				
Plano de continuidade de negócio				
Ensaios de continuidade de negócio e <i>disaster recovery</i>				
Incidente que impede o acesso ao edifício durante xxx dias				
Incidente que impede o acesso físico ao edifício				
Incidente que destrói o arquivo clínico e sala de sistemas				

Conformidades

Conformidade	Existem procedimentos documentados para a gestão de... S/N	Existem elementos dedicados para a gestão de... S/N	Existem registos de S/N	Observações
Identificação da legislação aplicável				
Garantia de conformidade para com a legislação aplicável ao negócio				
Regulamentação de controlos criptográficos (chaves publicas e privadas)				
Licenciamento de <i>software</i> e protecção de direito de autor				
Confidencialidade e privacidade em dados privados dos utentes				
Plano de auditorias internas				
Plano de auditorias externas				

ANEXO C

Gomes, R. J., Lapão, L.V. et al. (2008). "The Adoption of IT Security Standards in a Healthcare Environment." eHealth Beyond the Horizon – Get IT There S.K. Andersen et l. (Eds.) IOS Press, MIE 2008

ANEXO D

Lapão, L. V., Rebugue, A., Silva, M.S., Gomes, R. J. “ ITIL Assessment in a Healthcare Environment: The Role of IT Governance at Hospital São Sebastião”. Medical Informatics in a United and Healthy Europe K.-P. Adlassnig et al. (Eds.). IOS Press